Oracle® Communications Diameter Signaling Router

DSR Cloud Software Upgrade Guide Release 8.6.0.0.0 F55340-01

April 2022



Oracle® Communications Diameter Signaling Router, Cloud Software Upgrade User's Guide, Release 8.6.0.0.0

Copyright © 2011, 2022 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable: U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.

Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

My Oracle Support (MOS) (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html.

See more information on My Oracle Support (MOS).

Table of Contents

1.	Intro	troduction11		
	1.1	Purpo	se and Scope	11
		1.1.1	What is Not Covered by this Document	11
	1.2	Refere	ences	11
	1.3	Acron	yms	11
	1.4	Termi	nology	13
	1.5	How to	o Use this Document	14
		1.5.1	Executing Procedures	15
	1.6	Recor	nmendations	15
		1.6.1	Frequency of Health Checks	15
		1.6.2	Large Installation Support	15
		1.6.3	Logging of Upgrade Activities	15
	1.7	Warni	ngs, Cautions, and Notes	16
		1.7.1	Signaling Firewall	16
		1.7.2	Network IDIH Compatibility	16
		1.7.3	Review Release Notes	16
		1.7.4	Upgrade Check	17
2.	Gen	eral De	escription	17
	2.1	Suppo	orted Upgrade Paths to 8.6.0.0.0	17
	2.2	Geo-D	Diverse Site (Active/Standby/Spare PCA Configuration)	18
	2.3	Traffic	Management During Upgrade	18
	2.4	Autom	nated Site Upgrade	19
		2.4.1	Site Upgrade Execution	20
		2.4.2	Minimum Server Availability	24
		2.4.3	Site Upgrade Options	25
		2.4.4	Cancel and Restart Auto Site Upgrade	26
	2.5	Autom	nated Server Group Upgrade	29
		2.5.1	Cancel and Restart Automated Server Group Upgrade	29
		2.5.2	Site Accept	30
3.	Upg	rade P	lanning and Pre-Upgrade Procedures	31
	3.1	Requi	red Materials and Information	31
		3.1.1	Application ISO Image File/Media	32
		3.1.2	Logins, Passwords and Server IP Addresses	32
	3.2	Plan L	Jpgrade Maintenance Windows	35
		3.2.1	Calculating Maintenance Windows Required	36
	3.3	Site U	pgrade Methodology Selection	36

		3.3.1	DA-MP Upgrade Planning	39
		3.3.2	Pre-upgrade validation to avoid Comcol inter-connectivity issue between MPs	40
		3.3.3	Maintenance Window 1 (NOAM Site Upgrades)	41
		3.3.4	Maintenance Window 2 and Beyond (SOAM Site Upgrades)	41
	3.4	Prerec	quisite Procedures	45
		3.4.1	Required Materials Check	45
		3.4.2	DSR ISO Administration	47
		3.4.3	Data Collection — Verification of Global and Site Configuration Data	51
		3.4.4	Back Up TKLCConfigData Files	56
		3.4.5	Full Backup of DB Run Environment at Each Server	57
		3.4.6	IDIH Pre-Upgrade	60
	3.5	Softwa	are Upgrade Execution Overview	61
		3.5.1	Accepting the Upgrade	62
4.	NO	AM Upg	grade Execution	62
	4.1	NOAN	I Pre-Upgrade Checks and Backup	63
		4.1.1	NOAM Health Check for Source Release 8.0 and Later	64
		4.1.2	NOAM Pre-Upgrade Backup	67
	4.2	Disab	le Global Provisioning	68
	4.3	NOAN	1 Upgrade	69
	4.4	Verify	NOAM Post Upgrade Status	70
	4.5		Provisioning (Post NOAM Upgrade)	
5.	Site	Upgra	de Execution	73
	5.1	Site P	re-Upgrade Activities	73
		5.1.1	Site Pre-Upgrade Backups	74
		5.1.2	Site Pre-Upgrade Health Checks	77
		5.1.3	Site Upgrade Options Check	81
		5.1.4	Disable Site Provisioning	82
	5.2	Autom	nated Site Upgrade	83
		5.2.1	Site Upgrade Pre-Checks	83
		5.2.2	Initiate Automated Site Upgrade	84
		5.2.3	Rearrange Automated Site Upgrade Cycles	88
	5.3	Autom	nated Server Group/Manual Upgrade Overview	91
		5.3.1	Site Upgrade Planning	93
		5.3.2	SOAM Upgrade Overview	95
		5.3.3	Upgrade SOAMs	96
		5.3.4	Upgrade Iteration 3	98
		5.3.5	Upgrade Iteration 4	112

		5.3.6	Upg	grade Iteration 5	118
	5.4	Site P	ost-L	Jpgrade Procedures	120
		5.4.1	Allo	w Site Provisioning	120
		5.4.2	Site	Post-Upgrade Health Checks	120
		5.4.3	Pos	st-Upgrade Procedures	126
6.	Bac	kout P	roce	dure Overview	127
	6.1	Recov	/ery I	Procedures	129
	6.2	Backo	out H	ealth Check	129
	6.3	Disabl	le Gl	obal Provisioning	133
	6.4	Perfor	rm Er	mergency Backout	133
		6.4.1	Em	ergency Site Backout	133
		6.4.2	Em	ergency NOAM Backout	135
	6.5	Perfor	rm No	ormal Backout	137
		6.5.1	Nor	mal Site Backout	137
		6.5.2	Nor	mal NOAM Backout	141
	6.6	Back	Out S	Single Server	142
	6.7	Back	Out N	Multiple Servers	148
	6.8	Post-E	Back	out Health Check	156
	6.9	IDIH E	Backo	out	156
		6.9.1	Ora	cle Server Backout	156
		6.9.2	Med	diation and Application Server Backout	156
Ap	pend	lix A.	Pos	st Upgrade Procedures	157
	Арр	endix A	\.1 .	Accept Upgrade	157
	Арр	endix A	٨.2.	Undeploy ISO	159
	Арр	endix A	٨.3.	Post Upgrade Accept Procedures	160
Ар	pend	lix B.	Inc	rease Maximum Number of Open Files	161
Ар	pend	lix C.	Upę	grade Single Server – DSR 8.x	164
Ар	pend	lix D.	Upç	grade Multiple Servers – Upgrade Administration	170
Ар	pend	ix E.	IDI	H Upgrade at a Site	178
	Арр	endix E	E.1.	Upgrade Oracle Guest	179
	Арр	endix E	E.2.	Upgrade the Mediation and Application Guests	182
Ар	pend	lix F.	Alte	ernate Server Upgrade Procedures	183
	Арр	endix F	.1.	Alternate Pre-Upgrade Backup	183
	Арр	endix F	.2.	Server Upgrade Using platcfg	186
	Арр	endix F	.3.	Manual DA-MP (N+0) Upgrade Procedure	189
	Арр	endix F	4.	ASG SBR Upgrade Procedure	190
	Арр	endix F	.5.	Manual SBR Upgrade Procedure	190

Appendix G.	Exp	pired Password Workaround Procedure	194
Appendix G	6.1.	Inhibit Password Aging	194
Appendix G	6.2.	Enable Password Aging	196
Appendix G	6.3.	Password Reset	197
Appendix H.	Net	work IDIH Compatibility Procedures	198
Appendix I.	Rec	over From a Failed Upgrade	199
Appendix J.	Crit	ical and Major Alarms Analysis	204
Appendix K.	Add	ditional Backout Steps	215
Appendix L.	Add	ditional Post-Backout Steps	218
Appendix M.	Mai	nual Completion of Server Upgrade	220
Appendix N.	Ide	ntify the DC server	224
Appendix O.	Lim	itations of Automated Server Group and Automated Site Upgrade	226
Appendix P.	Ad	anced Health Check Procedure	228
Appendix Q.	Wo	rkaround to Resolve DB Site Replication Alarms	231
Appendix R.	Wo	rkaround to Resolve the Server HA Switchover Issue	232
Appendix S.	Wo	rkaround to Resolve Device Deployment Failed Alarm	233
Appendix T.	Wo	rkaround to Resolve syscheck Error for CPU Failure	235
Appendix U.	Cre	ate a Link for ComAgent	236
Appendix V.	Cha	ange SOAM VM Profile for Increased MP Capacity on an OpenStack system	237
Appendix W.	Cha	ange SOAM VM Profile for Increased MP Capacity on a VMware system	239
Appendix X.	Res	set the SOAP Password	242
Appendix Y.	Res	store the Servers with Backout Errors	244
Appendix Z.	Му	Oracle Support (MOS)	245

List of Tables

Table 1:	Acronyms	. 11
Table 2:	Terminology	. 13
Table 3.	Server Selection vs. Server Group Function	.23
Table 4.	Site Upgrade Availability vs. Server Group Function	.25
Table 5:	Logins, Passwords, and Server IP Addresses	. 32
Table 6.	Traffic Analysis Checklist	. 37
Table 7.	DA-MP Upgrade Planning Sheet	.40
Table 8.	Prerequisite Procedures Overview	.45
Table 9.	Release Specific Data Collection Procedures	. 52
Table 10	. IDIH Upgrade Preparation Overview	.60
Table 11	. NOAM Upgrade Execution Overview	. 62

Table 12.	Site Upgrade Execution Overview	73
Table 13.	Non-PCA/PDRA Site Upgrade Plan	92
Table 14.	Two-Site Redundancy PCA Site Upgrade Plan	92
Table 15.	Three-Site Redundancy PCA Site Upgrade Plan	92
Table 16.	Site Upgrade Planning Sheet	93
Table 17.	Site Upgrade Execution Overview	95
Table 18.	SOAM Upgrade Execution Overview	95
Table 19.	Iteration 3 Upgrade Execution Overview	98
Table 20.	Iteration 4 Upgrade Execution Overview.	112
Table 21.	Iteration 5 Upgrade Execution Overview	118
Table 22.	Emergency Backout Procedure Overview	127
Table 23.	Normal Backout Procedure Overview	128
Table 24.	IDIH Upgrade Execution Overview	178
Table 25.	High Impact Alarms	204
Table 26.	Medium Impact Alarms	208

List of Figures

Figure 1. Example Procedure Steps Used in This Document
Figure 2. DSR 8.6.0.0.0 Supported Upgrade Paths
Figure 3. Upgrade Perspective of DSR "Site" Topology
Figure 4. Site Upgrade – NOAM View
Figure 5. Site Upgrade - Entire Site View
Figure 6. Site Upgrade - Site Initiate Screen
Figure 7. Site Upgrade Monitoring
Figure 8. Server Group Upgrade Monitoring
Figure 9. Auto Site Upgrade General Options
Figure 10. Site Upgrade Active Tasks
Figure 11. Canceled Site Upgrade Tasks
Figure 12. Partially Upgraded Site
Figure 13. Restarting Site Upgrade
Figure 14. Active Tasks Screen
Figure 15. Site Accept Button
Figure 16. Site Accept Screen
Figure 17. Upgrade Maintenance Windows for 3-Tier Upgrade
Figure 18. Specialized Fixed Diameter Connections
Figure 19. Specialized Floating Diameter Connections

	Figure 20	Specialized Distribution of DSR Features	
--	-----------	--	--

List of Procedures

Procedure 1.	Required Materials Check	. 46
Procedure 2.	DSR ISO Administration	. 47
Procedure 3.	Verification of Configuration Data	. 51
Procedure 4.	Data Collection for Source Release 8.0 and Later	. 53
Procedure 5.	TKLCConfigData backup	. 57
Procedure 6.	Full Backup of DB Run Environment for Release 8.0.x and Later	. 58
Procedure 7.	IDIH Upgrade Preparation	. 61
Procedure 8.	NOAM Health Check for Source Release 8.0 or Later	. 64
Procedure 9.	NOAM Pre-Upgrade Backup	. 67
Procedure 10.	Disable Global Provisioning	. 68
Procedure 11.	NOAM Upgrade	. 69
Procedure 12.	Verify NOAM Post Upgrade Status	. 70
Procedure 13.	Allow Provisioning (Post NOAM Upgrade)	.72
Procedure 14.	Site Pre-Upgrade Backups	.74
Procedure 15.	Site Pre-Upgrade Health Check for Release 8.0 and Later	. 78
Procedure 16.	Site Upgrade Options Check	. 81
Procedure 17.	Disable Site Provisioning	. 82
Procedure 18.	Site Upgrade Pre-Checks	. 83
Procedure 19.	Automated Site Upgrade	. 84
Procedure 20.	Rearrangement of upgrade cycles for Automated Site Upgrade	. 88
Procedure 21.	SOAM Upgrade Pre-Checks	. 96
Procedure 22.	Automated SOAM Upgrade (Active/Standby)	. 97
Procedure 23.	Manual SOAM Upgrade (Active/Standby/Spare)	. 97
Procedure 24.	Upgrade Iteration 3	. 98
Procedure 25.	Upgrade Iteration 4	112
Procedure 26.	Upgrade Iteration 5	118
Procedure 27.	Allow Site Provisioning	120
Procedure 28.	Site Post-Upgrade Health Check	121
Procedure 29.	Alternate SOAM Post-Upgrade Health Check	124
Procedure 30.	Post-Upgrade Procedures	126
Procedure 31.	Backout Health Check	129
Procedure 32.	Disable Global Provisioning	133
Procedure 33.	Emergency Site Backout	134

Procedure 34.	Emergency NOAM Backout	135
Procedure 35.	Normal Site Backout	137
Procedure 36.	Normal NOAM Backout	141
Procedure 37.	Back Out Single Server	142
Procedure 38.	Back Out Multiple Servers	148
Procedure 39.	Post-Backout Health Check	156
Procedure 40.	Accept Upgrade	157
Procedure 41.	Undeploy ISO	159
Procedure 42.	Post Upgrade Accept Procedure	160
Procedure 43.	Increase Maximum Number of Open Files	161
Procedure 44.	Upgrade Single Server – Upgrade Administration – DSR 8.x	164
Procedure 45.	Upgrade Multiple Servers – Upgrade Administration	170
Procedure 46.	Upgrade Oracle Guest	179
Procedure 47.	Upgrade the Mediation and Application Guests	182
Procedure 48.	Alternate Pre-Upgrade Backup	183
Procedure 49.	Server Upgrade Using Platcfg	186
Procedure 50.	Manual DA-MP (N+0) Upgrade Procedure	189
Procedure 51.	ASG SBR Upgrade	190
Procedure 52.	Manual SBR Upgrade Procedure	190
Procedure 53.	Expired Password Workaround Procedure	195
Procedure 54.	Expired Password Workaround Removal Procedure	196
Procedure 55.	Expired Password Reset Procedure	197
Procedure 56.	Enable IDIH 8.x Compatibility	198
Procedure 57.	Disable IDIH 8.x Compatibility	198
Procedure 58.	Recover from a Failed Upgrade	199
Procedure 59.	Verify Critical and Major Alarms in the System Before the Upgrade	204
Procedure 60.	Additional Backout Steps for NOAM, SOAM, and SBR Server(s)	215
Procedure 61.	Additional Post Backout Steps for NOAM, SOAM, and SBR Server(s)	218
Procedure 62.	Manual Completion of Server Upgrade	220
Procedure 63.	Identification of the DC server	224
Procedure 64.	Firewall Check for DNS Port 53	228
Procedure 65.	Workaround to Resolve DB Site Replication Alarms	231
Procedure 66.	Resolve the HA Switchover Issue on Affected Server(s)	232
Procedure 67.	Resolve Device Deployment Failed Alarm	233
Procedure 68.	Workaround to Resolve syscheck Error for CPU Failure	235
Procedure 69.	Create a Link for ComAgent	236
Procedure 70.	Change SOAM VM Profile for Increased MP Capacity on an OpenStack system	237

Procedure 71.	Change SOAM VM Profile for Increased MP Capacity on a VMware system	239
Procedure 72.	Reset the SOAP Password	242
Procedure 73.	Restore the Servers with Backout Errors	244

1. Introduction

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to perform the following upgrades:

8.1.2, 8.2.1, 8.3, 8.3.X, 8.4, 8.4.0.X.Y, 8.5.X to 8.6.0.0.0.

X = PI End Cycle

Y = Patches within the PI Cycle.

The upgrade of cloud deployments is covered by this document. The audience for this document includes Oracle customers as well as following internal groups: Software Development, Quality Assurance, Information Development, and Consulting Services including NPx. This document provides instructions to execute any incremental or major cloud software upgrade.

The execution of this procedure assumes that the target DSR software load (ISO file, CD-ROM or other form of media) has already been delivered to the customer's premises. This includes delivery of the software load to the local workstation being used to perform this upgrade.

Note: To understand the capacity/performance impact of this software release, refer to the [8] DSR Cloud Benchmarking document.

1.1.1 What is Not Covered by this Document

The following items are beyond the scope of this document. Refer to the specified reference for additional information.

- Distribution of DSR 8.x software loads. It is recommended to contact My Oracle Support (MOS) for the software loads as described in Appendix Z.
- Initial installation of DSR software. Refer to [1].
- SDS installation. Refer to [2].

1.2 References

- [1] DSR Cloud Installation Guide
- [2] SDS Cloud Installation document
- [3] Maintenance Window Analysis Tool CGBU_010314
- [4] Fast Deployment and Configuration Tool Technical Reference, CGBU_ENG_24_2353
- [5] Cloud DSR Disaster Recovery Guide
- [6] Oracle Communications DSR Introducing SCTP Datagram Transport Layer Security (DTLS) In DSR By Enabling SCTP AUTH Extensions By Default, OSD 2019141.1
- [7] DSR Alarms and KPIs Reference
- [8] DSR Cloud Benchmarking document

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1: Acronyms

Acronym	Meaning
ASG	Automated Server Group upgrade

Acronym	Meaning
ASU	Automated Site Upgrade
CD-ROM	Compact Disc Read-only Media
СРА	Charging Proxy Agent
CSV	Comma-separated Values
DA	Diameter Agent
DA MP	Diameter Agent Message Processor
DB	Database
DP	Data Processor
DR	Disaster Recovery
DSR	Diameter Signaling Router
DSR DR NOAM	Disaster Recovery DSR NOAM
FABR	Full Address Based Resolution
FOA	First Office Application
GA	General Availability
GPS	Global Product Solutions
GUI	Graphical User Interface
НА	High Availability
IDIH	Integrated Diameter Intelligence Hub
IMI	Internal Management Interface
IP	Internet Protocol
IPM	Initial Product Manufacture
IPFE	IP Front End
ISO	ISO 9660 file system (when used in the context of this document)
LA	Limited Availability
MOP	Method of Procedure
MP	Message Processing or Message Processor
MW	Maintenance Window
NE	Network Element
NOAM	Network OAM
OAM	Operations, Administration and Maintenance
OFCS	Offline Charging Solution
PCA	Policy and Charging Agent (formerly known as PDRA)
PDRA	Policy Diameter Routing Agent
SBR	Session Binding Repository
SDS	Subscriber Database Server

Acronym	Meaning
SOAM	System OAM
TPD	Tekelec Platform Distribution
UI	User Interface
VIP	Virtual IP
VPN	Virtual Private Network
ХМІ	External Management Interface
XSI	External Signaling Interface
vSTP	Virtual Signaling Transfer Point

1.4 Terminology

This section describes terminology as it is used within this document.

Term	Definition
Upgrade	The process of converting an application from its current release on a system to a newer release.
Major Upgrade	An upgrade from one DSR release to another DSR release, e.g., DSR 8.0 to 8.2.
Incremental Upgrade	An upgrade within a given DSR release e.g. 8.2.x to 8.2.y.
Release	Release is any particular distribution of software that is different from any other distribution.
Source Release	Software release to upgrade from
Target Release	Software release to upgrade to
Single Server Upgrade	The process of converting a DSR 8.2 server from its current release to a newer release.
Backout	The process of converting a single DSR 8.2 server to a prior version. This could be performed due to failure in Single Server Upgrade or the upgrade cannot be accepted for some other reason. Backout is a user initiated process.
Rollback	Automatic recovery procedure that puts a server into its pre-upgrade status. This procedure occurs automatically during upgrade if there is a failure.
Primary NOAM Network Element	The network element that contains the active and standby NOAM servers in a DSR.
Signaling Network Element	Any network element that contains DA-MPs (and possibly other C-level servers), thus carrying out Diameter signaling functions. Each SOAM pair and its associated C-level servers are considered a single signaling network element. And if a signaling network element includes a server that hosts the NOAMs, that signaling network element is also considered to be the primary NOAM network element.
Site	Physical location where one or more network elements reside. The site is defined by the SOAM.

Table 2: Terminology

Term	Definition
Geographic Site	A Geographic Site is defined as the physical location of a SOAM and its co- located children, as well as its non-preferred spare SOAM(s). In this document, a Geographic Site is designated as GSite .
Topological Site	A Topological Site is defined as a SOAM Server Group and all C-level Server Groups that are children of the SOAM. All servers within a server group belong to the server group's site, regardless of the physical location of the server. Thus, for upgrade, a Topological Site does not correlate to a 'network element' or a 'place'. In this document, a Topological Site is designated as TSite .
Health Check	Procedure used to determine the health and status of the DSR's internal network. This includes status displayed from the DSR GUI and PM&C GUI. This can be observed pre-server upgrade, in-progress server upgrade, and post-server upgrade.
Upgrade Ready	 State that allows for graceful upgrade of a server without degradation of service. It is a state that a server is required to be in before upgrading a server. The state is defined by the following attributes: Server is Forced Standby
	Server is Application Disabled (signaling servers do not process any traffic)
UI	User interface. Platcfg UI refers specifically to the Platform Configuration Utility User Interface, which is a text-based user interface.
N+0	Set up with N active DA-MP(s), but no standby DA-MP.
NOAM	Network OAM for DSR.
SOAM	System OAM for DSR.
Migration	Changing policy and resources after upgrade (if required). For example, changing from 1+1 (active/standby) policy to N+ 0 (multiple active) policies.
Software Centric	The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware, and is not responsible for hardware installation, configuration, or maintenance.
Enablement	The business practice of providing support services (hardware, software, documentation, etc) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.

1.5 How to Use this Document

- 1. When executing the procedures in this document, there are a few key points which help to ensure that the user understands procedure convention. These points are: Before beginning a procedure, completely read the instructional text (it displays immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
- 2. Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.
- 3. If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP. It is recommended to contact My Oracle Support (MOS) for assistance, before attempting to continue.

1.5.1 Executing Procedures

Figure 1 shows an example of a procedural step used in this document.

- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 and step 2 and substep 2.1.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.
- GUI fields and values to take note of during a step are in bold Arial font.

Each step has a checkbox the user should check to keep track of the progress of the procedure. The Title column describes the operations to perform during that step. Each command the user enters, and any response output, is formatted in 10-point Courier font.

Title/Instructions	Directive/Result Steps
--------------------	------------------------

1.	Change directory	Change to the backout directory. \$ cd /var/TKLC/backout
2.	Verify Network Element data	 View the Network Elements configuration data; verify the data; save and print report. 1. Select Configuration > Network Elements to view Network Elements Configuration screen.

Figure 1. Example Procedure Steps Used in This Document

1.6 Recommendations

This section provides some recommendations to consider when preparing to execute the procedures in this document.

1.6.1 Frequency of Health Checks

The user may execute the **Perform Health Check** or **View Logs** steps repetitively between procedures during the upgrade process. It is not recommended to do this between steps in a procedure, unless there is a failure to troubleshoot.

1.6.2 Large Installation Support

For large systems containing multiple Signaling Network Elements, it is impossible to upgrade multi-site systems in a single maintenance window.

1.6.3 Logging of Upgrade Activities

It is a best practice to use a terminal session with logging enabled to capture user command activities and output during the upgrade procedures. These can be used for analysis in the event of issues encountered during the activity. These logs should be saved off line at the completion of the activity.

1.7 Warnings, Cautions, and Notes

This section presents notices of warnings and cautions that directly relate to the success of the upgrade. It is imperative that each of these notices be read and understood before continuing with the upgrade. If there are any conflicts, issues, or questions related to these notices, it is recommended to contact My Oracle Support (MOS) before starting the upgrade.

1.7.1 Signaling Firewall

Signaling firewall remains disabled when upgrade is done from Pre 8.x release to 8.x release. If there is need to enable the signaling firewall after upgrade to 8.x release, then there are some limitations.



After the upgrade to release 8.2, signaling firewall cannot be enabled when there is at least one SCTP multi-homed connection is enabled.

A **Cannot enable Signaling Firewall** error message displays when there is at least on SCTP multihomed connection.

Also, if the signaling firewall is enabled after the upgrade, the SCTP multi-homed connections cannot be enabled.

A SCTP Multi-homed connections cannot be enabled when Signaling Firewall is administratively enable error message displays.



After the upgrade to release 8.2, SCTP multi-homed connection cannot be enabled if signaling firewall is already enabled.

1.7.2 Network IDIH Compatibility

Upgrading an IDIH site to release 8.2.x makes it incompatible for viewing network trace data contained in remote IDIH sites that are running a prior release. The incompatibility is removed once all Network IDIH systems have been upgraded to release 8.2.x.

To view network traces for a network of IDIH systems where there is a mix of systems running release 8.2.x and systems running a prior release, Procedure 56 in Appendix H must be executed to prepare the systems running IDIH release 8.2.x to support IDIH systems running the prior release. After executing Procedure 56, network traces should be viewed only from an IDIH system running the prior IDIH release. Viewing a network trace from an IDIH 8.2.x results in a visualization that is incomplete because the IDIH 8.2.x system fails to retrieve Trace Transaction Records (TTRs) from IDIH systems running the prior IDIH release.

When all IDIH systems have been upgraded to release 8.2.x, Procedure 57 should be executed on each IDIH system where Procedure 56 was previously executed to ensure that no errors occur when viewing network traces.

1.7.3 Review Release Notes

Before starting the upgrade, it is recommended to review the Release Notes for the target release to understand the functional differences and possible traffic impacts of the upgrade.

1.7.4 Upgrade Check

			11	WARNIN	\G !!	!		
thi	s error displays,	, contac	t My Oracle Supp	oort (MOS).				
20:	-		ion failed fo	r <server_n< th=""><th>ame>.</th><th>Please</th><th>check se</th><th>rve</th></server_n<>	ame>.	Please	check se	rve
tat	tus. Cancel	ling t	the upgrade."					
tai	tus. Cancel	ling t	The upgrade."	e Pinto-SQ-Sp Runtarq-SER-1	Mustang-SBR-2	Mustang SBR-3 Pinlo-0	569-1 Pinto-SER-2 Pint	6.8
ta Ta	_	-		p Pinto SO Sp Ministerg SBB 1 Update Time	Mustang-SBR-2 Reset	Nustang SBR-3 Proto Result Details	SBR-1 Prop-SBR-2 Pert Progress	66
ta fer	_	Mustarp-WP2	Parto-4P1 Perto-4P2 (Mustang-5D-5)	CONTRACTOR OF THE REAL	Number 2 SBR 2 Result	Nexturg SSR-3 Pinto 4 Result Details Server upgrade execution complete		60



CAUTION If your deployment includes both FABR and PCA, then upgrade the DSR nodes first before upgrading the SDS nodes.

2. General Description

This document defines the step-by-step actions performed to execute an upgrade of an in-service DSR from the source release to the target release. A major upgrade advances the DSR from source release 8.0 to target release 8.6.0.0.0. An incremental upgrade advances the DSR from an earlier DSR 8.5.X source release to a more recent 8.6.0.0.0 target release.

Note: With any incremental upgrade, the source and target releases must have the same value of **x**. For example, advancing a DSR from 8.4.0.0.0-84.5.0 to 8.5.0.0.0_90.11.0 is an incremental upgrade. But, advancing a DSR running 8.0 release to an 8.6.0.0.0 target release constitutes a major upgrade.

2.1 Supported Upgrade Paths to 8.6.0.0.0

The supported paths to upgrade to a DSR 8.6.0.0.0 target release are shown in Figure 2.

Note: DSR upgrade procedures assume the source and target releases are the GA or LA builds in the upgrade path.

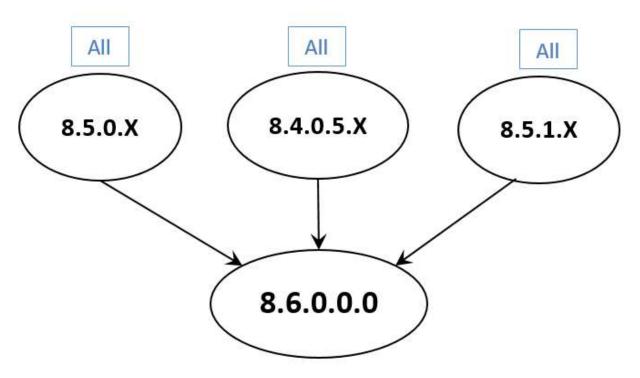


Figure 2. DSR 8.6.0.0.0 Supported Upgrade Paths

X = PI End Cycle

Y = Patches within the PI Cycle.

2.2 Geo-Diverse Site (Active/Standby/Spare PCA Configuration)

With a geo-diverse site, the upgrade of the SOAM active/standby servers must also include an upgrade of the spare SOAM at the geo-redundant site, in the same maintenance window.

2.3 Traffic Management During Upgrade

The upgrade of the NOAM and SOAM servers is not expected to affect traffic processing at the DA-MPs and other traffic-handling servers.

For the upgrade of the DA-MPs and IPFEs, traffic connections are disabled only for the servers being upgraded. The remaining servers continue to service traffic.



Oracle introduced SCTP Datagram Transport Layer Security (DTLS) in DSR 8.0 by enabling SCTP AUTH extensions by default. SCTP AUTH extensions are required for SCTP DTLS. However, there are known impacts with SCTP AUTH extensions as covered by the CVEs referenced in [6]. It is highly recommended that customers upgrading to Release 8.6.0.0.0 should prepare clients before the DSR is upgraded. This ensures the DSR-to-Client SCTP connection establishes with DTLS with SCTP AUTH extensions enabled.

If customers DO NOT prepare clients to accommodate the DTLS changes, then the SCTP connections to client devices DO NOT restore after the DSR is upgraded to DSR 8.6.0.0.0. In the event that the SCTP connections do not re-establish after the upgrade, follow the Disable/Enable DTLS procedure in [1].

2.4 Automated Site Upgrade

There are multiple methods available for upgrading a site. The newest and most efficient way to upgrade a site is the Automated Site Upgrade feature. As the name implies, this feature upgrades an entire site (SOAMs and all C-level servers) with a minimum of user interaction. Once the upgrade is initiated, the upgrade automatically prepares the server(s), performs the upgrade, and sequences to the next server or group of servers until all servers in the site are upgraded. The server upgrades are sequenced in a manner that preserves data integrity and processing capacity.

Automated Site Upgrade can be used to upgrade the DSR servers. However, Auto Site Upgrade cannot be used to upgrade IDIH servers at a site.

An important definition with regard to a site upgrade is the **site**. For the purposes of DSR site upgrade, a **site** is defined as a SOAM server group plus all subtending servers of that server group, **regardless of physical location**. To demonstrate this definition, Figure 3 shows three physical locations, labeled **TSite 1**, **TSite 2**, and **TSite 3**. Each site contains a SOAM server group and an MP server group. Each SOAM server group has a spare SOAM that, although physically located at another site, is a member of the site that "owns" the server group. With site upgrade, SOA-Sp is upgraded with the Site 1 SOA server group, and SOB-sp is upgraded with the Site 2 SOB server group. The MP server groups are upgraded in the same maintenance window as their respective site SOAMs. These sites conform to the Topological Site definition of Table 2: Terminology.

- 1. With this feature, a site upgrade can be initiated on SO-A SG and all of its children (in this example, MP1 SG) using a minimum of GUI selections. The upgrade performs the following actions: Upgrade SOA-1, SOA-2, and SOA-sp.
- 2. Upgrade the servers in MP1 SG based on an availability setting and HA roles.
- 3. Immediately begin the upgrade of any other server groups which are also children of SO-A SG (not shown). These upgrades begin in parallel with step 2.

Server groups that span sites (e.g., SOAMs and SBRs) are upgraded with the server group to which the server belongs. This results in upgrading spare servers that physically reside at another site, but belong to a server group in the SOAM that is targeted for site upgrade.

Note: Automated Site Upgrade does not automatically initiate the upgrade of TSite 2 in parallel with TSite 1. However, the feature does allow the user to initiate Auto Site Upgrade of multiple sites in parallel **manually**.

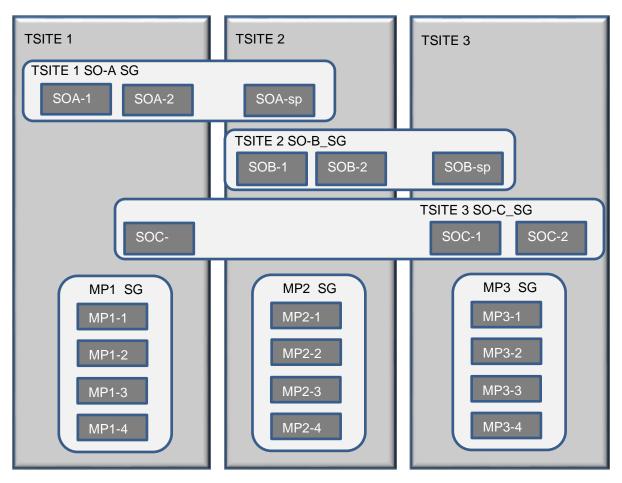


Figure 3. Upgrade Perspective of DSR "Site" Topology



Limitations in Appendix U for Automated Site Upgrade can be solved by rearranging/adding the upgrade cycles. If the user does not want to create a custom upgrade plan by rearranging/adding cycles then in that case manual upgrade section 5.3 method should be used

2.4.1 Site Upgrade Execution

CAUTION

With Auto Site Upgrade, the upgrade is initiated from the **Administration > Software Management > Upgrade** GUI. Upon initial entry to this screen, the user is presented with a tabbed display of the NOAM server group and SOAM sites (Figure 4). When the NOAM server group tab is selected (as shown in Figure 4), this screen is largely unchanged from the upgrade screen of previous releases. The NOAM server group servers are displayed with the usual assortment of buttons. On this screen, **Auto Upgrade** refers to Automated Server Group upgrade, not Automated Site Upgrade. The site upgrade feature becomes available once a SOAM server group tab is selected. The SOAM server group tabs correspond to the topological sites (TSites).

Filter* ▼ Tasks ▼					W
NO_SG SO_East	SO_North SO_Wes	st			
Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
nosulaille	Server Status	Appl HA Role	Network Element	Network Element	
NOD	Ready	Active	Network OAM&P	OAM&P	8.0.0.0-80.18.0
NO2	Norm N/A NO_DSR_VM				
	Ready	Standby	Network OAM&P	OAM&P	8.0.0.0-80.18.0
NO1	Norm	N/A	NO DSR VM		

Figure 4. Site Upgrade – NOAM View

After selecting a SOAM site tab on the Upgrade Administration screen, the site summary screen is displayed (Figure 5). Just below the row of NOAM and SOAM tabs is a row of links related to the selected SOAM site. The first link on the site summary screen displays the Entire Site view. In the entire site view, all of the server groups for the site are displayed in table form, with each server group populating one row. An upgrade summary of the server groups is provided in the table columns:

- The Upgrade Method column shows how the server group is upgraded. The upgrade method is derived from the server group function and the bulk availability option (see Section 2.4.3 for additional details on bulk availability).
- The Server Upgrade States column groups the servers by state, indicating the number of servers in the server group that are in each state.
- The Server Application Versions column indicates the current application version, indicating the number of servers in the server group that are at each version.

Ford_NO_SG Chevy_DRNO	_SG Camam_SO_SG Mestang_SO_SG	Nova_80_9G Pinte_80_9G		
Entro Ste Musling_50_55	Musling_NP_SG Musling_SBR_SG1	Westing_SUR_992		
Server Group	Function	Upgrade Method	Server Upgrade States	Server Application Version
Mustang_SO_SG	DSR (active/standby pair)	OAM (Bulk)	Ready (3r3)	8 1.0.0.0-81 20.0 (3/3)
Nustang_SER_SG1	SBR	Serial	Ready (3/3)	8.1.0.0 0-81.20 0 (3/3)
Nustang_SBR_SG2	SBR	Serial	Ready (3/3)	8.1.0.0.0-81.20.0 (3/3)
Mustang_MP_SG	DSR (multi-active cluster)	Bulk (50% availability)	Ready (2/2)	8.1.0.0.0-81.20.0 (2/2)
Mustang_MP_SG	DSR (multi-active cluster)	Bulk (50% availability)	Ready (207)	8.1.0.0.0-81.20.0 (2/2)

Figure 5. Site Upgrade - Entire Site View

For a server to be considered "Ready" for upgrade, the following conditions must hold true:

- Server has not been upgraded yet
- The FullDBParts and FullRunEnv backup files exist in the filemgmt area

A site is eligible for Automated Site Upgrade when at least one server in the site is upgrade-ready.

Click **Site Upgrade** from the **Entire Site** screen to display the Upgrade Site Initiate screen (Figure 6). The **Site Initiate** screen presents the site upgrade as a series of upgrade cycles. For the upgrade shown in Figure 6, Cycle 1 upgrades the spare and standby SOAMs in parallel.

- *Note*: This scenario assumes default settings for the site upgrade options. These options are described in Section 2.4.3.) The specific servers to be upgraded in each cycle are identified in the **Servers** column of the **Site Initiate** display. Cycle 1 is an atomic operation, meaning that Cycle 2 cannot begin until Cycle 1 is complete. Once the spare and standby SOAMs are in **Accept or Reject** state, the upgrade sequences to Cycle 2 to upgrade the active SOAM. Cycle 2 is also atomic Cycle 3 does not begin until Cycle 2 is complete.
- **Note:** IPFE servers require special handling for upgrade, because IPFE servers are clustered into Target Sets and assigned an IP address, it is called Target Set Assignment (TSA). While upgrading IPFE servers, Auto Site Upgrade makes sure that there is no service outage for IPFE while upgrade is in progress, that is, IPFE servers in same TSA are not upgraded in same cycle. If IPFE server address is not configured on **IPFE -> Configuration -> Options** screen on active SOAM GUI, that IPFE server are not included in the Upgrade Cycle; therefore, are not considered for upgrade using Automated Site Upgrade.

		Server Group	Server	Function		Method	Version	
	Upgrade	Mustang_SO_SG	Pinto-SO-Sp - Spare Mustang-SO-B - Standby		'standby pair) OAM (Bulk	8.1.0.0.0-	
		Server Group	Server	Function		Method	Version	
	Upgrade	Mustang_SO_SG	Mustang-SO-A - Active	DSR (active/st	tandby pair)	OAM (Bulk)	8.1.0.0.0-8	1.20.0
		Server Group	Server	Function		Method		Version
3	Upgrade	Mustang_MP_SG	Mustang-MP1		tive cluster)	Bulk (50% av		3.1.0.0.0-81.20.0 3.1.0.0.0-81.20.0
		Manufacture and a second second	2 Pinto-SBR-6 - Spare			Serial		3.1.0.0.0-81.20.0
		Server Group	Server	Function	n	Metho	t	Version
		Mustang_MP_SG	Mustang-MP2	DSR (mu	ilti-active clu	ster) Bulk (5	0% availabil	ity) 8.1.0.0.0-81.20.
	Upgrade	Mustang_SBR_SG	Mustang-SBR-1 - Stan	dby SBR		Serial		8.1.0.0.0-81.20
		Mustang_SBR_SG	2 Mustang-SBR-5 - Star	idby SBR		Serial		8.1.0.0.0-81.20
		Server Group	Server	Function	Method	Version		
8	Upgrade	Mustang_SBR_SG	1 Mustang-SBR-2 - Acti	ve SBR	Serial 1	3.1.0.0.0-81.2	0.0	
		Mustang_SBR_SG	2 Mustang-SBR-4 - Actu	Ve SBR	Serial I	3.1.0.0.0-81.2	0.0	
lpgrade Set	tings							
In second s 1800	- Select - 💌	Select the desired u	upgrade ISO media file.					
Jpgrade ISO								

Main Menu: Administration -> Software Management -> Upgrade [Site Initiate]

Figure 6. Site Upgrade - Site Initiate Screen

Cycles 3 through 5 upgrade all of the C-level servers for the site. These cycles are **not** atomic.

In Figure 6, Cycle 3 consists of IPFE1, IPFE3, MP1, MP4, and SBR3. Because some servers can take longer to upgrade than others, there may be some overlap in Cycle 3 and Cycle 4. For example, if IPFEs 1 and 3 complete the upgrade before SBR3 is finished (all are in Cycle 3), the upgrade allows IPFEs 2

and 4 to begin, even though they are part of Cycle 4. This is to maximize Maintenance Window efficiency. The primary factor for upgrading the C-level servers is the upgrade method for the server group function (for example, bulk by HA, serial, etc.).

The site upgrade is complete when every server in the site is in the Accept or Reject state.

In selecting the servers that are included with each upgrade cycle, particularly the C-level, consideration is given to the server group function, the upgrade availability option, and the HA designation. Table 3 describes the server selection considerations for each server group function.

Note: The minimum availability option is a central component of the server selections for site upgrade. The effect of this option on server availability is described in detail in Section 2.4.2.

SG Function	Selection Considerations
DSR (multi-active cluster) (for example, DA-MP)	The selection of servers is based primarily on the minimum server availability option. Servers are divided equally (to the extent possible) among the number of cycles required to enforce minimum availability. For DA-MPs, an additional consideration is given to the MP Leader. The MP with the Leader designation is the last DA-MP to be upgraded to minimize leader changes ¹ .
DSR (active/standby pair) (for example, SOAM)	The SOAM upgrade method is dependent on the Site SOAM Upgrade option on the General Options page. See section 2.4.3.
SBR	SBRs are always upgraded serially, thus the primary consideration for selection is the HA designation. The upgrade order is spare – spare – standby – active.
IP Front End	IPFEs require special treatment during upgrade. One consideration for selection is the minimum server availability, but the primary consideration is traffic continuity. Regardless of minimum availability, IPFE A1 is never upgraded at the same time as IPFE A2. They are always upgraded serially. The same restriction applies to IPFE B1 and B2. If minimum availability permits, IPFE A1 can be upgraded with IPFE B1, and IPFE A2 can be upgraded with B2.

Table 3. Server Selection vs. Server Group Function

¹ In the event of a leader change while upgrades are in progress, the MP Leader may not be the last MP to be upgraded.

To initiate the site upgrade, a target ISO is selected from the ISO picklist in the **Upgrade Settings** section of the **Site Initiate** screen (Figure 6). Once the **OK** button is clicked, the upgrade starts, and control returns to the Upgrade Administration screen (Figure 7). With the **Entire Site** link selected, a summary of the upgrade status for the selected site is displayed. This summary identifies the server group(s) currently upgrading, the number of servers within each server group that are upgrade status of the overall site. More detailed status is available by selecting the individual server group links. The server group view shows the status of each individual server within the selected server group.

Filter* ▼ Tasks	-			
NO_SG SO_East	SO_North SO_West st IPFE1_SG IPFE2_SG IPF	E3_SG IPFE4_SG MP_S	G	
Server Group	Function	Upgrade Method	Server Upgrade States	Server Application V
SO_East	DSR (active/standby pair)	OAM (Bulk)	Pending (1/2) Upgrading (1/2)	7.2.0.0.0-72.25.0 (2/2)
IPFE2_SG	IP Front End	Serial	Pending (1/1)	7.2.0.0.0-72.25.0 (1/1)
MP_SG	DSR (multi-active cluster)	Bulk (50% availability)	Pending (2/4)	7.2.0.0.0-72.25.0 (4/4)

Figure 7. Site Upgrade Monitoring

When a server group link is selected on the upgrade administration screen, the table rows are populated with the upgrade details of the individual servers within that server group (Figure 8).

	Iministration -> S	oftware Mana	igement -> Up	grade	Tue Jan 03 16:
Filter* Status					
NO_SG SO East	t SO_North SO_Wes	t			
Entire Site SO Fa	ast IPFE1_SG IPFE2	2 SG IPFE3 SG	IPFE4 SG MP	96	
Entire Site	ast herei_30 ierez	2_30 IFFE3_30	IFFE4_30 WIF_		
	Ungrado State	OAM HA Role	Server Role	Function	A surflow Allow Mountain
Hostnamo	Upgrade State	OAIII HA ROIC	Server Kole	Function	Application Version
Hostname	Server Status	Appl HA Role	Network Element		Upgrade ISO
Hostname SO1	Server Status	Appl HA Role	Network Element	t	Upgrade ISO
	Server Status Pending	Appl HA Role Active	Network Element	t	Upgrade ISO 7.2.0.0.0-72.25.0

Figure 8. Server Group Upgrade Monitoring

Upon completion of a successful upgrade, every server in the site is in the **Accept** or **Reject** state. See Section 2.4.3 for a description of canceling and restarting the Automated Site Upgrade.

2.4.2 Minimum Server Availability

The concept of Minimum Server Availability plays a key role during an upgrade using Automated Site Upgrade. The goal of server availability is to ensure that at least a specified percentage of servers (of any given type) remain in service to process traffic and handle administrative functions while other servers are upgrading.

For example, if the specified minimum availability is 50% and there are eight servers of type X, then four remain in service while four upgrade. However, if there are nine server of type X, then the minimum availability requires that five remain in service while four upgrade. The minimum availability calculation automatically rounds up in the event of a non-zero fractional remainder.

To meet the needs of a wide-ranging customer base, the minimum availability percentage is a userconfigurable option. The option allows for settings of 50%, 66%, and 75% minimum availability. There is also a setting of 0% for lab upgrade support. This option is described in detail in Section 3.3.

The application of minimum server availability differs for the various server group functions. For some function types, it is a straight calculation of a percentage. However, for others, minimum availability does

not apply due to overriding operational considerations. Table 4 describes the application of availability for the various server group functions.

Server Group Function	Server Availability
DSR (multi-active cluster)	In a multi-active cluster, the availability percentage applies to all of the servers in the server group. The number of servers required to achieve minimum availability are calculated from the pool of in-service servers.
SBR	Availability percentage does not apply to SBR server groups. SBRs are upgraded in a very specific order: spare – spare – standby – active
IP Front End	IPFEs require special treatment during upgrade. The primary consideration is traffic continuity. Regardless of minimum availability, IPFE A1 is never upgraded at the same time as IPFE A2. They are always upgraded serially. The same restriction applies to IPFE B1 and B2.

Table 4. Site Upgrade Availability vs. Server Group Function

When calculating the number of servers required to satisfy the minimum server availability, all servers in the server group (or server group cluster) are considered. Servers that are OOS or otherwise unable to perform their intended function, are included, as are servers that have already been upgraded. For example, consider a DA-MP server group with 10 servers; four have already been upgraded, one is OOS, and five are ready for upgrade. With a 50% minimum availability, only four of the servers that are ready for upgrade in parallel. The four servers that have already been upgraded count toward the five that are needed to satisfy minimum availability. The OOS server cannot be used to satisfy minimum availability, thus leaving four servers to be upgraded together. Upgrading the last server would require an additional upgrade cycle.

2.4.3 Site Upgrade Options

To minimize user interactions, the automated site upgrade makes use of a pair of pre-set options to control certain aspects of the sequence. These options control how many servers remain in service while others are upgrading and are located on the **Administration > General Options** screen (Figure 9). The default settings for these options maximize the maintenance window usage by upgrading servers in parallel as much as possible.

Site Upgrade Bulk Availability *	1	Site based upgrade availability for bulk upgrade of MP groups. (0 = none, 1 = 50%, 2 = 66%, 3 = 75%). ** Cannot be changed while any site upgrade is running. ** [Default = 1; Range = 0-3] [A value is required.]
Site Upgrade SOAM Method *	1	Site based upgrade SOAM method. (0 = serial, 1 = bulk). <u>Note:</u> Bulk upgrade will upgrade all non-active SOAM servers together. ** Cannot be changed while any site upgrade is running. ** [Default = 1; Range = 0-1] [A value is required.]

Figure 9. Auto Site Upgrade General Options

The first option that affects the upgrade sequence is the **Site Upgrade SOAM Method**. This option determines the sequence in which the SOAMs are upgraded. The default value of 1 considers the OAM HA role of the SOAMs to determine the upgrade order. In this mode, all non-active SOAM servers are upgraded first (in parallel), followed by the active SOAM. This upgrade method requires at most two

upgrade cycles to upgrade all of the SOAMs, regardless of how many are present. If there are no spare SOAMs, then this setting has no effect on the SOAM upgrade.

Regardless of the SOAM upgrade method, the active SOAM is always upgraded after the standby and spare SOAMs.

The second option that affects the upgrade sequence is the **Site Upgrade Bulk Availability** setting. This setting determines the number of C-level servers that remain in service during the upgrade. The default setting of "1" equates to 50% availability, meaning that a minimum of one-half of the servers stay in service during the upgrade. The default setting is the most aggressive setting for upgrading the site, requiring the minimum number of cycles, thus the least amount of time. The settings of 66% and 75% increase the number of servers that remain in service during the upgrade.

Note: Increasing the availability percentage may increase the overall length of the upgrade.

The application of minimum server availability varies for the different types of C-level servers. For example, for a multi-active DA-MP server group, the minimum availability applies to all of the DA-MPs within the server group. This same setup applies to IPFEs as well. Table 4 defines how the Site Upgrade Bulk Availability setting on the General Options page affects the various server group function types.

The Site Upgrade General Options cannot be changed while a site upgrade is in progress. Attempting to change either option while a site upgrade is in progress results in:

```
[Error Code xxx] - Option cannot be changed because one or more automated site upgrades are in progress
```

2.4.4 Cancel and Restart Auto Site Upgrade

When an Auto Site Upgrade is initiated, several tasks are created to manage the upgrade of the individual server groups as well as the servers within the server groups. These tasks can be monitored and managed via the Active Task screen (**Status & Manage > Tasks > Active Tasks**).

The main site upgrade controller task is identified by the naming convention **<site_name> Site Upgrade**. In Figure 10, the main task is task ID 22. This task is controlling the server group upgrade task (task ID 23), which in turn is controlling the server upgrade task (task ID 24).

Filte	r* 🔻					102	Jan 03 17:43:12 2017
NO1	NO2 SO1 SO2	MP1 MF	2 IPFE1 IPFE2 IPF	E3 IPFE4 MP3 MP4	SBR	81	
D	Name	Status	Start Time	Update Time	Result	Result Details	Progress
24	SO1 Server Upgrade (in SO_East Server Group Upgrade)	running	2017-01-03 17:40:27 UTC	2017-01-03 17:42:02 UTC	0	Upgraded server to new ISO	90%
23	SO_East Server Group Upgrade (in SO_East Site Upgrade)	running	2017-01-03 17:40:18 UTC	2017-01-03 17:40:27 UTC	0	Upgrade(s) started.	5%
22	SO_East Site Upgrade	running	2017-01-03 17:40:10 UTC	2017-01-03 17:40:18 UTC	0	Upgrade(s) started.	5%

Figure 10. Site Upgrade Active Tasks

To cancel the site upgrade, select the site upgrade task and click **Cancel**. A screen requests confirmation of the cancel operation. The status changes from **running** to **completed**. The Results Details column updates to display **Site upgrade task cancelled by user**. All server group upgrade tasks that are under the control of the main site upgrade task immediately transition to **completed** state. However the site upgrade cancellation has no effect on the individual server upgrade tasks that are in

progress. These tasks continue until completion. Figure 11 shows the Active Task screen after a site upgrade has been canceled.

Once the site upgrade task is canceled, it cannot be restarted. However, a new site upgrade can be started via the Upgrade Administration screen.

Filte	il _* ▲						Jan 03 18:13:17 2017
NO	1 NO2 SO1 SO2	MP1 MP2	IPFE1 IPFE2 IPFE	E3 IPFE4 MP3 MP4	SBF	81	
ID	Name	Status	Start Time	Update Time	Result	Result Details	Progress
30	SO2 Server Upgrade (in SO_East Server Group Upgrade)	running	2017-01-03 18:11:06 UTC	2017-01-03 18:13:06 UTC	0	Upgraded server to new ISO	90%
29	SO_East Server Group Upgrade (in SO_East Site Upgrade)	completed	2017-01-03 18:10:57 UTC	2017-01-03 18:12:59 UTC	0	SG upgrade task cancelled by user.	5%
28	SO East Site Upgrade	completed	2017-01-03 18:10:48 UTC	2017-01-03 18:12:59 UTC	0	Site upgrade task cancelled by user.	5%

Figure 11. Canceled Site Upgrade Tasks

Figure 12 is representative of a site upgrade that was canceled before the site was completely upgraded. The servers that were in progress when the upgrade was canceled continued to upgrade to the target release. These servers are now in the Accept or Reject state. The servers that were pending when the upgrade was canceled are now in the Ready state, ready to be upgraded.

To restart the upgrade, verify the **Entire Site** link is selected and click **Site Upgrade**. The Upgrade Site Initiate screen displays.

Camaro_S0_SG DSR (adiversitandby pair) OAM (Bulk) Accept or Reject (30) 82.00.0	
	Application Version
2000 001 000 000 000 0000 0000 00000 00000 00000	82.6.0 (3/3)
Caman_SBR_SG1 SBR Senal Accept or Reject (33) 0.2.0.0	-82.6.0 (3/3)
Camaro_SBR_SG2 BBR Serial Ready (35) #1.0.0.0	61 20 0 (3/3)
Camaro_MP_9G DOR (multi-active cluster) Bulk (59% availability) Accept or Reject (2/2) 8 2.0.0	-82.6.0 (2/2)

Figure 12. Partially Upgraded Site

On the Upgrade Site Initiate screen, the servers that have not yet been upgraded are grouped into the number of cycles that are required to complete the site upgrade. For the upgrade that was canceled in Figure 11, only a single cycle is needed since the availability requirements can be met by the servers that have already been upgraded. Once an ISO is selected and **OK** is clicked, the site upgrade continues normally.

Info* 👻								
Cycle	Action	Servers						
		Server Group	Server	Functio	on Me	thod '	Version	
1	Upgrade	Camaro_SBR_SG2	Nova-SBR-6 - Spare	SBR	Sei	rial 8	3.1.0.0.0-81.20.0	
2		Server Group	Server	Fi	Inction	Meth	od Version	
2	Upgrade	Camaro_SBR_SG2	Camaro-SBR-4 - Star	ndby SE	BR	Serial	8.1.0.0.0-81.2	20.0
3	the same dia	Server Group	Server	Fun	ction	Method	Version	
2	Upgrade	Camaro_SBR_SG2	Camaro-SBR-5 - Act	Ve SBF	2	Serial	8.1.0.0.0-81.20	.0
Upgrade Se	ettings							
Upgrade IS	0 - Select - 💌	Select the desired up	grade ISO media file.					
Cancel	Rearrange Cycles	Report						

Figure 13. Restarting Site Upgrade

2.5 Automated Server Group Upgrade

The Automated Server Group (ASG) upgrade feature allows the user to upgrade all of the servers in a server group automatically by specifying a set of controlling parameters.

The purpose of ASG is to simplify and automate segments of the DSR upgrade. The DSR has long supported the ability to select multiple servers for upgrade. In doing so however, it was incumbent on the user to determine ahead of time which servers could be upgraded in parallel, considering traffic impact. If the servers were not carefully chosen, the upgrade could adversely impact system operations.

When a server group is selected for upgrade, ASG upgrades each of the servers serially, or in parallel, or a combination of both, while enforcing minimum service availability. The number of servers in the server group that are upgraded in parallel is user selectable. The procedures in this document provide the detailed steps specifying when to use ASG, as well as the appropriate parameters that should be selected for each server group type.

ASG is the default upgrade method for most server group types associated with the DSR. However, there are some instances in which the manual upgrade method is utilized. In all cases where ASG is used, procedures for a manual upgrade are also provided.

Note: To use ASG on a server group, no servers in that server group can be already upgraded – either by ASG or manually.

DSR continues to support the parallel upgrade of server groups, including any combination of automated and manual upgrade methods.

2.5.1 Cancel and Restart Automated Server Group Upgrade

When a server group is upgraded using ASG, each server within that server group is automatically prepared for upgrade, upgraded to the target release, and returned to service on the target release. Once an ASG upgrade is initiated, the task responsible for controlling the sequencing of servers entering upgrade can be manually canceled from the **Status & Manage > Active Tasks** screen (Figure 14) if necessary. Once the task is cancelled, it cannot be restarted. However, a new ASG task can be restarted via the Upgrade Administration screen.

For example, in Figure 14, task ID #1 (SO_SG Server Group Upgrade) is an ASG task, while task ID #2 is the corresponding individual server upgrade task. When the ASG task is selected (highlighted in green), the **Cancel** button is enabled. Canceling the ASG task affects only the ASG task. It has no effect on the individual server upgrade tasks that were started by the ASG task (that is task ID #2 in Figure 14). Because the ASG task is canceled, no new server upgrades are initiated by the task.

	ain Menu: Status & Manage -> Tasks -> Active Tasks					
NO1		MP2 IPFE				
ID	Name	Status	Start Time	Update Time		
2	SO1 Server Upgrade (in SO_SG Server Group Upgrade)	running	2015-03-02 11:44:42 EST	2015-03-02 11:54:00 EST		
1	SO_SG Server Group Upgrade	running	2015-03-02 11:44:32 EST	2015-03-02 11:47:47 EST		
0	Pre-upgrade full backup	completed	2015-02-27 19:59:06 EST	2015-02-27 20:00:46 EST		
Pause	Restart Cancel Delete R	eport Delete All C	Completed Delete All Exception			

Figure 14. Active Tasks Screen

In the event that a server fails upgrade, that server automatically rolls back to the previous release in preparation for backout_restore and fault isolation. Any other servers in that server group that are in the process of upgrading continue to upgrade to completion. However, the ASG task itself is automatically cancelled and no other servers in that server group are upgraded. Cancelling the ASG task provides an opportunity for troubleshooting to correct the problem. Once the problem is corrected, the server group upgrade can be restarted by initiating a new server group upgrade on the upgrade screen.

2.5.2 Site Accept

The **Site Accept** button on the upgrade GUI (Figure 15) provides the capability to nearly simultaneously accept the upgrade of some or all servers for a given site. When the button is clicked, a subsequent screen (Figure 16) displays the servers that are ready for the Accept action.



Figure 15. Site Accept Button

A checkbox on the Upgrade Site Accept screen allows for the selective application of the Accept action. However, normal procedure calls for the Accept to be applied to all of the servers at a site only after the upgrade to the new release is stable and the back out option is no longer needed. After verifying that the information presented is accurate, clicking **OK** results in a screen that requires confirmation of the intended action. Confirming the action causes the server upgrades to be accepted.

The Accept command is issued to the site servers at a rate of approximately one server every second. The command takes approximately 10 seconds per server to complete. As the commands are completed, the server status on the Upgrade Administration screen transitions to **Backup Needed**.

Main Menu	: Administrat	tion -> Software Managen	nent -> Upgrade [Site Accept]
Server group	Action	Server(s) which are Pending Accept	
SO_East	Accept upgrade	SO1 SO2	
IPFE_\$G1	✓ Accept upgrade	IPFE1	
IPFE_\$G2	Accept upgrade	IPFE2	
IPFE_\$G3	Accept upgrade	IPFE3	
IPFE_\$G3	Accept upgrade	IPFE4	
MP_SG	Accept upgrade	MP4 MP1 MP2 MP3	
SBR_SG	Accept upgrade	SBR1 SBR2 SBR3	
Ok Cance	I		

Figure 16. Site Accept Screen

3. Upgrade Planning and Pre-Upgrade Procedures

This section contains all information necessary to prepare for and execute an upgrade. The materials required to perform an upgrade are described, as are pre-upgrade procedures that should be run to ensure the system is fully ready for upgrade. Then, the actual procedures for each supported upgrade path are given.

There are overview tables throughout this document that help plan the upgrade and estimate how long it takes to perform various actions. The stated time durations for each step or group of steps **are estimates only**. Do not use the overview tables to execute any actions on the system. Only the procedures should be used when performing upgrade actions, beginning with Procedure 1.



For vSTP-related deployments, it is not allowed to do any adding/updating/deleting of configuration until the upgrade is completed on all sites and the upgrade is accepted.

Note: While planning an upgrade, be aware that once the upgrade is started and OAM level servers are on different releases than servers on different sites, OAM level provisioning data is not replicated to sites that have not been upgraded.

Once servers at the site are upgraded, replication from OAM level serves is restored and upgraded servers start receiving provisioning data.

Read 2.4 Automated Site Upgrade for details and limitations/solutions while planning upgrade cycles.

There are some limitations with upgrading the DC server in a C-level server group that are upgraded in a group of servers, for example DA-MP, vSTP MP(s). So, while manually upgrading, make sure the DC server is not upgraded in the first upgrade cycle of the C-Level servers in its server group. Identify the DC server using Appendix N Identify the DC server.

In all cases, regardless of the number of cycles used to upgrade the DA-MP/vSTP server group, the DA-MP leader/vSTP MP leader should be the last server upgraded. By upgrading the MP leader last, the number of leader changes is minimized during the upgrade.

The DA-MP leader is designated on the active SOAM at **Diameter > Maintenance > DA-MPs > Peer DA-MP Status**, where **MP Leader = Yes**.

Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI.

1. From the MMI command using the REST Client for the vSTP configuration.

The MMI user guide can accessed by navigating to **Main Menu > MMI Guide**.

2. Use the /vstp/mpleader MO.

The result is the hostname of the MP leader server.

Note: If the **31149 - DB Late Write Nonactive** displays, ignore it. This alarm does not have any effect on functionality.

3.1 Required Materials and Information

The following materials and information are needed to execute an upgrade:

- Target-release application ISO image file or target-release application media.
- The capability to log into the network OAM servers with administrator privileges.
 - *Note*: All logins into the DSR NOAM servers are made using the external management VIP unless otherwise stated.
- User logins, passwords, IP addresses and other administration information. See [Table 5].

VPN access to the customer's network is required if that is the only method to log into the OAM servers.

3.1.1 Application ISO Image File/Media

Obtain a copy of the target release ISO image file or media. This file is necessary to perform the upgrade.

The DSR ISO image file name is in the following format (version changes from release to release):

DSR-DSR-8.6.0.0.0 95.14.0-x86 64.iso

Note: Before the execution of this upgrade procedure it is assumed that the DSR ISO image file has already been delivered to the customer's premises. The ISO image file must reside on the local workstation used to perform the upgrade, and any user performing the upgrade must have access to the ISO image file. If the user performing the upgrade is at a remote location, it is assumed the ISO file is already available before starting the upgrade procedure.

The ISO is deployed as part of the pre-upgrade activities in Section 3.4.

3.1.2 Logins, Passwords and Server IP Addresses

Table 5 identifies the information that is called out in the upgrade procedures, such as server IP addresses and login credentials. For convenience, space is provided in Table 5 for recording the values, or the information can be obtained by other means. This step ensures that the necessary administration information is available before an upgrade.

Consider the sensitivity of the information recorded in this table. While all of the information in the table is required to complete the upgrade, there may be security policies in place that prevent the actual recording of this information in hard-copy form.

Item	Description	Recorded Value
Target Release	Target DSR upgrade release	
Credentials	GUI Admin Username ¹	
	GUI Admin Password	
	DSR admusr Password ²	
	DSR Root Password ²	
VPN Access Details	Customer VPN information (if needed)	

Table 5: Logins, Passwords, and Server IP Addresses

¹ The user must have administrator privileges. This means the user belongs to the **admin** group in Group Administration.

² This is the password for the server login. This is not the same login as the GUI Administrator. The admusr password is required if recovery procedures are needed. If the admusr password is not the same on all other servers, then all those servers' admusr passwords must also be recorded; use additional space at the bottom of this table.

Item	Description	Recorded Value
NOAM	XMI VIP address ³	
	NOAM 1 XMI IP Address	
	NOAM 2 XMI IP Address	
SOAM	XMI VIP address	
	SOAM 1 XMI IP Address (Site 1)	
	SOAM 2 XMI IP Address (Site 1)	
	PCA (DSR) Spare System OAM&P server – Site 1 Spare in Site 2, XMI IP Address	
	SOAM 1 XMI IP Address (Site 2)	
	SOAM 2 XMI IP Address (Site 2)	
	PCA (DSR) Spare System OAM&P server – Site 2 Spare in Site 1, XMI IP Address	
Binding SBR Server	Binding SBR SR1 Server Group Servers (Site 1)	
Groups	Binding SBR SR2 Server Group Servers (Site 1)	
	Binding SBR SR3 Server Group Servers (Site 1)	
	Binding SBR SR4 Server Group Servers (Site 1)	
PCA MP Server Group	PCA MP Server Group Servers (Site 1)	
	PCA MP Server Group Servers (Site 1)	
IPFE Server Groups(For PDRA)	PCA IPFE A1 Server Group Server (Site 1)	
	PCA IPFE A 2 Server Group Server (Site 1)	
	PCA IPFE B 1 Server Group Server (Site 1)	
	PCA IPFE B 2 Server Group Server (Site 1)	
Binding SBR Server	Binding SBR SR1 Server Group Servers (Site 2)	
Groups	Binding SBR SR2 Server Group Servers (Site 2)	
	Binding SBR SR3 Server Group Servers (Site 2)	
	Binding SBR SR4 Server Group Servers (Site 2)	
PCA MP Server Group	PCA MP Server Group Servers (Site 2)	
	PCA IPFE A1 Server Group Server (Site 2)	

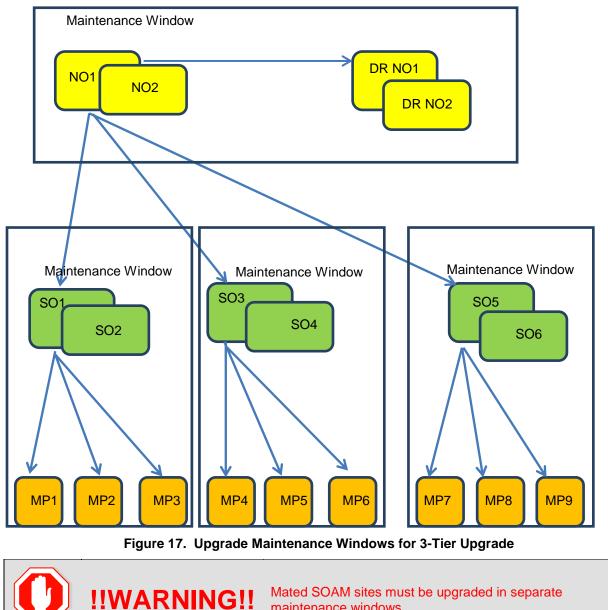
³ All logins into the NOAM servers are made via the External Management VIP unless otherwise stated.

ltem	Description Recorded Value		
IPFE Server Groups (For PCA)	PCA IPFE A 2 Server Group Server (Site 2)		
	PCA IPFE B 1 Server Group Server (Site 2)		
	PCA IPFE B 2 Server Group Server (Site 2)		
vSTP MP Server Group	vSTP MP server(s)		
Software	Target Release Number		
	ISO Image (.iso) file name		
Misc. ⁴	Miscellaneous additional data		

⁴ As instructed by Oracle CGBU Customer Service.

3.2 Plan Upgrade Maintenance Windows

This section provides a high-level checklist to aid in tracking individual server upgrades. The servers are grouped by maintenance window, and it is expected that all servers in a group can be successfully upgraded in a single maintenance window. Use this high-level checklist together with the detailed procedures that appear later in this document.



maintenance windows.

Page | 35

3.2.1 Calculating Maintenance Windows Required

The number of maintenance windows required for DSR setup and upgrade can be calculated by using the Maintenance Window Analysis Tool (see ref [3]).

This Excel spreadsheet takes setup details as input from the user and accordingly calculates the number of maintenance windows required for upgrade. The spreadsheet also specifies, in detail, which servers need to be upgraded in which maintenance window. Complete DSR upgrade maintenance window details and timings can be found in Reference [3]. Please see the instructions tab of the spreadsheet for more information and details.

3.3 Site Upgrade Methodology Selection

There are three primary methods for upgrading a DSR site:

- Auto Site Upgrade
- Auto Server Group Upgrade
- Manual upgrade

The Auto Site Upgrade is the easiest and most efficient site upgrade method; however, it is not suitable for all customers or all configurations. The Auto Server Group upgrade incorporates many of the conveniences of Auto Site Upgrade, but allows for more customer control of the upgrade process.

The Automated Site Upgrade supports 0% availability that requires the least amount of time to upgrade the sites. This can be achieved by changing the following parameters:

Site Upgrade SOAM Method setting to **0** - Changing the Site Upgrade SOAM Method setting to 0 causes the standby SOAM and the spare SOAM(s) to be upgraded serially. With this mode, the SOAM upgrade could take as many as four cycles to complete (that is, spare – spare – standby – active). If there are no spare SOAMs, then this setting has no effect on the SOAM upgrade.

Site Upgrade Bulk Availability setting to **0** - Changing the Site Upgrade Bulk Availability setting to 0 equates to 0% availability that means no servers are required to stay in service during the upgrade. This setting requires the minimum number of cycles, thus the least amount of time. This setting allows all of the DA-MPs to be upgraded at once.

Site Upgrade Bulk Availability *	0	Site based upgrade availability for bulk upgrade of MP groups. (0 = none, 1 = 50%, 2 = 66%, 3 = 75%). ** Cannot be changed while any site upgrade is running. ** [Default = 1; Range = 0-3] [A value is required.]
Site Upgrade SOAM Method *	0	Site based upgrade SOAM method. (0 = serial, 1 = bulk). <u>Note:</u> Bulk upgrade will upgrade all non-active SOAM servers together. ** Cannot be changed while any site upgrade is running. ** [Default = 1; Range = 0-1] [A value is required.]

Again, Auto Server Group upgrade is not for all customers or all configurations. The manual upgrade method gives maximum control to the customer and can be used for all configurations. A combination of upgrade methods can be utilized to upgrade a given site to maximize efficiency with customer peace-of-mind.

Table 6 is a worksheet for determining which upgrade method meets the needs of the customer while ensuring compatibility with the DSR configuration. Upon completion of the worksheet, a recommended upgrade method is identified.

	Criteria	Yes	No	Notes	
1.	Do any of the site's DA-MPs have fixed diameter connections to any peer node, similar to this depiction?			Automated Site Upgrade and Automated Server Group upgrade, by default, do not consider fixed peer connections when selecting servers to upgrade. It is possible that all DA-MPs servicing a given peer (such as DA-MPs 1 and 3) could be upgraded simultaneously, thereby isolating the peer. For this reason, analyze the generic upgrade plan generated by the Automated Site Upgrade and Auto Server Group Upgrade carefully to ensure all DA-MPs servicing a given peer are not upgraded simultaneously. If the generic plan has the DA-MPs upgrading simultaneously, you must rearrange the upgrade and/or add cycles as necessary to develop a suitable plan. If yes, proceed to section 5.2.3 to rearrange or add cycles for ASU or proceed to step 8 for a manual upgrade. If no, continue with step 2.	
2.	If peer nodes are configured via IPFE TSAs, are there any TSAs that are not distributed across all DA-MPs, similar to this depiction?			Automated Site Upgrade and Automated Server Group upgrade, by default, do not consider non-uniformly distributed TSAs when selecting servers to upgrade. It is possible that all DA-MPs servicing a given TSA (such as DA-MPs 1 and 2) could be upgraded simultaneously, thereby isolating the peer. For this reason, analyze the generic upgrade plan generated by the Automated Site Upgrade and Auto Server Group Upgrade carefully to ensure all DA-MPs servicing a given TSA are not upgraded simultaneously. If the generic plan has the DA-MPs upgrading simultaneously, you must rearrange the upgrade and/or add cycles as necessary to develop a suitable plan. If yes, proceed to section 5.2.3 to rearrange or add cycles for ASU or proceed to step 8 for a manual upgrade. If no, continue with step 3.	

Table 6. Traffic Analysis Checklist

	Criteria	Yes	No	Notes
3.	 3. Do any of the site's DA-MPs have specialized distribution of DSR features, similar to this depiction? DA-MP Server Group RBAR RBAR PDRA DCA DCA Only DCA PDRA PDRA Only DCA Peer RBAR Peer 4. Automated Site Upgrade is a candidate for 			Automated Site Upgrade and Automated Server Group upgrade, by default, do not consider non-uniform distribution of features when selecting servers to upgrade. It is possible that all DA-MPs hosting a given feature (such as DCA) could be upgraded simultaneously, thereby eliminating service functionality. For this reason, analyze the generic upgrade plan generated by the Automated Site Upgrade and Auto Server Group Upgrade carefully to ensure all DA-MPs hosting a given feature are not upgraded simultaneously. If the generic plan has the DA-MPs upgrading simultaneously, you must rearrange the upgrade and/or add cycles as necessary to develop a suitable plan. If yes, proceed to section 5.2.3 to rearrange or add cycles for ASU or proceed to step 8 for manual upgrade. If no, continue with step 4.
4.	Automated Site Upgrade is a candidate for this system. Automated Site Upgrade supports 50% minimum server availability by default. A general option allows availability percentage settings of 66% or 75%. Is 50%, 66%, or 75% server availability during upgrade acceptable to the customer?			In general, a higher minimum availability setting increases the time required to upgrade a site. On the other hand, a lower minimum availability may reduce operational redundancy during the upgrade. If none of the minimum availability options are acceptable, Automated Site Upgrade should not be used to upgrade the site. If yes, continue with step 6. If no, proceed to step 7.
5.	Is the customer comfortable with minimum user intervention (that is, user input) during the upgrade?			Once initiated, Automated Site Upgrade requires no additional user input to complete the upgrade. User control is limited to canceling the site upgrade task. If yes, Automated Site Upgrade is the recommended upgrade method. If no, proceed to step 7.
6.	Automated Server Group Upgrade is a candidate for this system. Is the customer comfortable with the level of control afforded by the Automated Server Group upgrade?			Auto Server Group upgrade allows the user to initiate the upgrade of each server group, while the individual servers within the server group upgrade automatically. If yes, Auto Server Group upgrade is the recommended upgrade method. If no, proceed to step 8.

	Criteria	Yes	No	Notes
7.	A manual upgrade affords the maximum level of control over upgrade sequencing. With this method, the upgrade of each server is individually initiated, allowing the user to control the level of parallelism and speed of the upgrade.			A manual upgrade is the recommended upgrade method.
	<i>Note</i> : A site upgrade can include a combination of Automated Server Group upgrade and manual upgrades to improve efficiency. For example, SBRs can be upgraded with Automated Server Group upgrade, while the DA-MPs may be upgraded manually to control the order of upgrade for traffic continuity.			

3.3.1 DA-MP Upgrade Planning

If a manual upgrade is recommended by the Table 6 worksheet, additional planning is required to ensure a successful upgrade of the DA-MP server group. A manual upgrade is typically required/recommended when the DA-MPs are configured in a way such that an upgrade could result in a traffic outage. Preplanning the upgrade of the DA-MPs is key to avoiding an outage.

Note: If complete site upgrade is selected with 0% availability then DA-MP upgrade planning is not required.

Table 7 is an aid to laying out the sequence of the DA-MP upgrades, taking into consideration configuration and traffic continuity. **This worksheet must be completed by the customer and provided to Oracle if Oracle personnel are performing the upgrade**. It is highly recommended that the worksheet be completed for customer-driven upgrades as well.

Customer: Perform an analysis of the Diameter application and connection configurations to assess any potential traffic loss due to the DA-MP upgrade. Complete the worksheet, specifying the order in which the DA-MPs will be upgraded, and which MPs, if any, can be upgraded in parallel.

The worksheet is divided into four upgrade **Cycles**. Each cycle represents an upgrade period during which one or more servers are upgraded. Distributing the DA-MPs servers over two or more cycles, takes advantage of parallels, thereby reducing the time required to upgrade the entire server group.

To achieve 50% server availability, half of hostnames would be listed in Cycle 1 while the other half would be listed in Cycle 2, requiring two upgrade cycles. Similarly, 75% availability can be achieved by spreading the hostname over all four cycles.

In all cases, regardless of the number of cycles used to upgrade the DA-MP/vSTP server group, the DA-MP leader/vSTP MP leader should be the last server upgraded. By upgrading the MP leader last, the number of leader changes is minimized during the upgrade.

The DA-MP leader is designated on the active SOAM at **Diameter > Maintenance > DA-MPs > Peer DA-MP Status**, where **MP Leader = Yes**.

Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI.

1. From the MMI command using the REST Client for the vSTP configuration.

The MMI user guide can accessed by navigating to **Main Menu > MMI Guide**.

2. Use the /vstp/mpleader MO.

The result is the hostname of the MP leader server.

Note: If desired, the DA-MPs can be upgrade serially, in which case, all hostnames would be listed in cycle 1. List the DA-MPs in the order in which they will be upgraded.

	Hostnames			
Upgrade Cycle 1 or				
Serial Upgrade				
	Hostna	imes		
Upgrade Cycle 2				
	Hostna	ames		
Upgrade Cycle 3				
	Hostna	imes		
Upgrade Cycle 4				
DA-MP Leader:				

Table 7.	DA-MP	Upgrade	Planning	Sheet
		opgraao	i iaining	011000

3.3.2 Pre-upgrade validation to avoid Comcol inter-connectivity issue between MPs

The HA framework enhancements cause the inter-connectivity issue between the old-DC and non-DC MP nodes during upgrade scenario.

Note: This procedure provides solution to resolve the inter-connectivity issue between the old-DC and non-DC MP at the time of upgrade for the BUG 27428669.

To overcome the inter-connectivity issue:

1. Check the Designated Coordinator (DC) node in the system by using the command:

ssh admusr@<MP server>

\$ ha.info -d

Example output:

```
Node ID: HDBDBGTGCHBDRA54TK
Report Time: 01/07/2018 03:48:43.299
***
DC: HDBDBGTGCHBDRA54TK Generation: 1 State: DC
Elected: 01/07/2018 02:14:40.822
Other Non-DC Group Members:
HDBDBGTGCHBDRA53TK
HDBDBGTGCHBDRA53TK
HDBDBGTGCHBDRA5BTK
HDBDBGTGCHBDRA5CTK
DC Group Candidates: <none>
```

- Before starting the MP server upgrade, disable the DSR application on current DC node, using command:
 - a. On Active SOAM Go to Server under Status & Manage option.
 - b. Disable the DSR application by selecting the MP (DC Node) and click Stop.
- 3. Select an MP to be upgraded:
 - Note: The MP Leader Node should be the last server to be upgraded.
 - Case where there existing IPFE based floating (Diameter) connections, choose an MP from TSA having more than 2 MPs.
 - **Note**: If there exists a TSA with just two MPs, and one having DC role. We should avoid using other MP (non-DC) in this TSA for upgrade at this step.
 - b. Case where there are MP based (Diameter) connection, select any MP except the MP having DC role.
- 4. After upgrade, one of the upgraded MP with new release takes over the new-DC role.
- 5. The DSR application remains disabled on the old-DC node, as performed in step 2.
- 6. The old-DC is upgraded in the next upgrade cycle.
- Once the upgrade is completed, from Active SOAM Go to Server under Status & Manage GUI screen and check if the DSR application is ENABLED on MP node (old-DC). If not then ENABLE it by restart button.

3.3.3 Maintenance Window 1 (NOAM Site Upgrades)

During the first maintenance window, the NOAM servers are upgraded.

Maintenance Window 1 (NOAM Sites)	Record the Site NE Name of the DSR NOAM to be upgraded during Maintenance Window 1 in the space provided below: " Check off " the associated Check Box as upgrade is completed for each server.
Date: Note: The NE Name may be viewed from the DSR NOAM GUI under Configuration ->	DR Standby NOAM (Guest): DR Active NOAM (Guest): Primary Standby NOAM (Guest): Drimary Active NOAM (Guest):
Network Elements.	Primary Active NOAM (Guest):

3.3.4 Maintenance Window 2 and Beyond (SOAM Site Upgrades)

During Maintenance Window 2, all servers associated with the first SOAM site are upgraded. All servers associated with the second SOAM site are upgraded during Maintenance Window 3.

For DSRs configured with multiple mated-pair sites, or DSRs having multiple, distinct sites (e.g., georedundant PCA installations), copy and use the following form for the subsequent SOAM site upgrades. From release 8.1, vSTP MP support is available. While upgrading from pre 8.1 releases, vSTP MP server will not be in the system. So, after major upgrade is completed. In case vSTP MP server is required, it is freshly installed on 8.1 release using reference [1]. For release 8.1, planning should be done for vSTP MP incremental upgrades.

Note: In release 8.1, there can be only one vSTP MP server in the STP server group and one server in one site. This means whenever the vSTP MP server is upgraded, there is traffic loss on that vSTP MP server.

	NING!! Mated SOAM sites must be upgraded in separate maintenance windows.
Maintenance Window SOAM Sites Date:	 Record the site NE Name of the DSR SOAM and the MP(s) to be upgraded during Maintenance Window 2 in the space provided. Mark the associated checkbox as each server upgrade is completed. SOAM Site:
	Active SOAM (Guest): DA-MP1: DA-MP2: DA-MP3: DA-MP3: DA-MP4: DA-MP5: DA-MP6: DA-MP7:
	DA-MP8: DA-MP9: DA-MP10: DA-MP11: DA-MP11: DA-MP12: DA-MP13: DA-MP14: DA-MP15: DA-MP16:

IPFE1:	
Binding Server Group 1 Standby SBR: Active SBR: Spare SBR1 (Mate): Spare SBR2 (Mate): Binding Server Group 2 Standby SBR:	(If equipped)
 Active SBR:	(If equipped)
Spare SBR1 (Mate): Spare SBR2 (Mate): Binding Server Group 4 Standby SBR: Active SBR:	(If equipped)
Spare SBR1 (Mate): Spare SBR2 (Mate): Binding Server Group 5 Standby SBR: Active SBD:	(If equipped)
Spare SBR1 (Mate): Spare SBR2 (Mate): Binding Server Group 6 Standby SBR:	(If equipped)
 Active SBR:	(If equipped)
Spare SBR1 (Mate):	

Spare SBR2 (Mate): Binding Server Group 8 Standby SBR:	
Active SBR:	
Spare SBR1 (Mate):	
☐ Spare SBR2 (Mate):	
Session Server Group 1	
Standby SBR:	
Active SBR:	
Spare SBR1 (Mate):	
Spare SBR2 (Mate):	(If equipped)
Session Server Group 2	
Standby SBR:	
Active SBR:	
Spare SBR1 (Mate):	
Spare SBR2 (Mate):	(If equipped)
Session Server Group 3	
Standby SBR:	
Active SBR:	
Spare SBR1 (Mate):	
Spare SBR2 (Mate):	(If equipped)
Session Server Group 4	
Standby SBR:	
Active SBR:	
Spare SBR1 (Mate):	
Spare SBR2 (Mate):	(If equipped)
Session Server Group 5	
Standby SBR:	
Active SBR:	
Spare SBR1 (Mate):	
Spare SBR2 (Mate):	(If equipped)
Session Server Group 6	
Standby SBR:	
Active SBR:	
Spare SBR1 (Mate):	
Spare SBR2 (Mate):	(If equipped)
Session Server Group 7	
Standby SBR:	

Active SBR:	_ (If equipped)
vSTP MP Server Group	_ (If equipped)

3.4 **Prerequisite Procedures**

The pre-upgrade procedures shown in the following table are executed outside a maintenance window, if desired. These steps have no effect on the live system and can save upon maintenance window time, if executed before the start of the Maintenance Window.

Procedure	Elapsed Time (hr:min)		Procedure Title
	This Step Cum.		
Procedure 1	0:10-0:30	0:10-0:30	Procedure 1 Required Materials Check
Procedure 2	0:15-0:30	0:25-1:00	Procedure 2 DSR ISO Administration
Procedure 3	0:20-0:30 0:55-1:30		Procedure 3 Verification of Configuration Data
Procedure 4	0:15-0:20	1:10-1:50	Procedure 4 Data Collection for Source Release 8.0 and Later
Procedure 5	0:15-0:30	1:30-3:05	Procedure 5 TKLCConfigData backup
Procedure 6	0:10-2:00	1:40-5:05	Procedure 6 Full Backup of DB Run Environment for Release 8.0.x and Later.

 Table 8. Prerequisite Procedures Overview

¹ ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. These factors may significantly affect total time needed, and may require the scheduling of multiple maintenance windows to complete the entire upgrade procedure. The ISO transfers to the target systems should be performed prior to, and outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

3.4.1 Required Materials Check

This procedure verifies that all required materials needed to perform an upgrade have been collected and recorded.

Procedure 1. Required Materi	als Check
------------------------------	-----------

Step #	Procedure	Description			
 This procedure verifies all required materials are present. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance. 					
1.	Verify all required materials are present	Materials are listed in Section 3.1: Required Materials. Verify required materials are present.			
2.	Verify all administration data needed during upgrade	Double-check that all information in Section 3.2 is filled-in and accurate.			
3.	Contact My Oracle Support (MOS)	It is recommended to contact My Oracle Support (MOS) and inform them of plans to upgrade this system. See Appendix Z for these instructions. <i>Note</i> : Obtaining a new online support account can take up to 48 hours.			

3.4.2 DSR ISO Administration

This section provides the steps to upload the new DSR ISO to the NOAMs and then transfer the ISO to all servers to be upgraded.

Note: ISO transfers to the target systems may require a significant amount of time depending on the number of systems and the speed of the network. These factors may significantly affect total time needed and require the scheduling of multiple maintenance windows to complete the entire upgrade procedure. The ISO transfers to the target systems should be performed before, and outside of, the scheduled maintenance window. Schedule the required maintenance windows accordingly before proceeding.

Step #	Procedure	Description
	off (\checkmark) each step as	ISO Administration steps have been completed. it is completed. Boxes have been provided for this purpose under each step
If this pr	ocedure fails, it is r	ecommended to contact My Oracle Support (MOS) and ask for assistance.
1. □	Active NOAM VIP: Transfer via NOAM GUI	Use the NOAM GUI upload function for ISO file transfer over the network. Upload the target release ISO image file to the File Management Area of the active NOAM server:
		1. Log into the active NOAM GUI.
		2. Navigate to Status & Manage > Files.
		3. Click the active NOAM server in the network to display all files stored in the file management storage area of this server.
		4. Ensure that this is actually the active NOAM server in the network by comparing the hostname in the screen title vs. the hostname in the session banner in the GUI. Verify they are the same and the status is Active in the session banner.
		5. Click Upload .
		Note: Actual screens may vary from those shown depending on the browser and browser version used.
		File: Upload Cancel

Step #	Procedure	Description
Step # 2.	Procedure Active NOAM VIP	Description 1. Click Browse to select the file to upload. 2. Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image file and click Open. Image: Select the target release ISO image image. Image: Select the target release ISO image im
3.	Active NOAM CLI: Change Permission of ISO	<pre>network upload speed is slow. Log into the Active NOAM CLI and execute the following command: sudo chmod 644 /var/TKLC/db/filemgmt/<dsr_iso_filename></dsr_iso_filename></pre>

Step #	Procedure	Description
4.	Active NOAM	1. Navigate to Status & Manage > Files.
	VIP: Using NOAM GUI,	2. Click the active NOAM server tab.
	deploy ISO to all servers to be	All files stored in the file management storage area of this server display on the screen.
	upgraded.	3. Select the target release ISO, and click View ISO Deployment Report.
		 In the resulting report, determine if the ISO has been deployed to all servers in the system.
		 If the ISO has been deployed to all servers, this procedure is complete. Proceed to the next procedure per Table 8.
		 If the ISO has not been deployed, select the target release DSR ISO in the file list, and click Validate ISO. Click OK on the confirmation screen.
		 Verify the ISO status is valid. If the ISO is not valid, repeat this procedure beginning with step 1. If the ISO fails validation more than once, it is recommended to contact My Oracle Support (MOS).
		8. If the ISO is valid, select the ISO, and click Deploy ISO . Click OK on the confirmation screen.
		Main Menu: Status & Manage -> Files
		Filter* ▼ Tasks ▼
		NO1 SO1
		File Name
		Backup.DSR.NO1.FullDBParts.NETWORK_OAMP.20180406_032543.UPG.tar.bz2
		Backup.DSR.NO1.FullRunEnv.NETWORK_OAMP.20180406_032543.UPG.tar.bz2 DSR-8.3.0.0.0_83.3.7-x86_64.iso
		TKLCConfigData.NO1.sh
		The cooling but an on the second seco
		Delete View ISO Deployment Report Upload Download Deploy ISO Validate ISO
		Are you sure you want to validate DSR-8.3.0.0.0_83.3.7-x86_64.iso?
		OK Cancel

Step #	Procedure	Description						
5.	Active NOAM VIP: Monitor	The deploymen on the Status 8				l by vie	wing the T a	asks options
	ISO deployment	Fitter* + Status +	Tasks	•				
			Tasks					0
		NO1 SO1 NO2	iD (II)	Hostname	Name	Task State	Details	Progress
		File Name Backup DSR NO2 FulDBF	139	502	190 Transfer 0SR- 8.3.0.0.0_83.3.7- x56_64 iso from so1-imi	completed	Done	10036
		Backup DSR NO2 FullRun backup Backup dtr NO2 C	•	NO1	190 Tratsfer DSR- 8.3.0.0.83.3.7- x86_64 iso from mo2-imi	completed	Dane	100%
		hackup/Backup dor NO2 C backup/Backup dor NO2 C	100	801	ISO Transfer DSR- 8 3 0 0 0 83 3 7-	comoletert	Done	100%
		Select the targe Verify the ISO h						
			nas	been dep	loyed to all ser	vers in	the system	
		Verify the ISO h	nas	been dep	loyed to all ser anage -> Files	vers in s [Viev	the system	
		Verify the ISO h	nas	been dep	loyed to all ser anage -> Files Main Menu: S	vers in s s [View status a	the system	> Files [View]
		Verify the ISO f	nas Stat	been dep tus & Ma	loyed to all ser anage -> Files Main Menu: S	s [View tatus apr 10 (the system Manage -: 01:35:34 20	> Files [View]
		Verify the ISO f	nas Stat	been dep tus & Ma	Nain Menu: S Tue J	s [View tatus apr 10 (the system Manage -: 01:35:34 20	> Files [View]
		Verify the ISO f Main Menu: S Deployment re Deployed on 4	nas Stat	been dep tus & Ma	Nain Menu: S Tue J	s [View tatus apr 10 (the system Manage -: 01:35:34 20	> Files [View]
		Verify the ISO F	por 4/4	been dep tus & Ma	Nain Menu: S Tue J	s [View tatus apr 10 (the system Manage -: 01:35:34 20	> Files [View]
		Verify the ISO f Main Menu: \$ Deployment re Deployed on 4 NO1: Deployed	por i/4 i	been dep tus & Ma	Nain Menu: S Tue J	s [View tatus apr 10 (the system Manage -: 01:35:34 20	> Files [View]

3.4.3 Data Collection — Verification of Global and Site Configuration Data

The procedures in this section are part of software upgrade preparation and are used to collect data required for network analysis, disaster recovery, and upgrade verification. Data is collected from both the active NOAM and various other servers at each site.

3.4.3.1 Verification of Configuration Data

This procedure checks the configuration data of the system and servers to ensure a successful upgrade.

Procedure 3. Verification of Configuration Data

Step #	Procedure	Description	Description				
This pro	cedure checks the	e configuration	data and serve	r status.			
Check o number.	ff ($√$) each step as	s it is complete	d. Boxes have	been provide	ed for this pur	pose une	der each step
If this pr	ocedure fails, it is	recommended	to contact My 0	Dracle Suppo	ort (MOS) and	d ask for	assistance.
1.	Active NOAM VIP: Verify application version	2. Verify th	e to Administra t e upgrade path on 2.1 (Supporte	to the target	release is su		
		120020-0202	ne NOAM Serve				Version.
		Filter + Task		ontinal e mana	gement - opg	nuuc	
		NOSG SOSO					
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade iSO
		N02	Ready	Active N/A	Network OAM&P	OAM&P	8.0.0.0.0-80.25.0
		NO1	Ready Norm	Standby N/A	Network OAM&P	OAM&P	8.0.0.0-80.25.0
2.	Active NOAM CLI: Check if the setup has customer supplied Apache certificate installed and protected with a passphrase	 windows ssh ad passwo Answer 2. cd to /et 3. Locate t 4. The path certificat the certi 	yes if you are as c/httpd/conf.d a he line beginning n that follows SS e. If the path is ficate is supplied	active NOAN TP> r passwor sked to confi and open the g with the ph LCertificate /usr/TKLC/a by Oracle a	d> rm the identity file named s rase SSLCer File is the loc appworks/etc	y of the s sl.conf. tificateF cation of c/ssl/ser	server. File. the Apache rver.crt, then
		5. If the pa /usr/TK Apache	e with the next s th is anything ot _C/appworks/e t certificate is like certificate pathna	her than t c/ssl/serve t ly installed.	Rename the	certificat	

The following data collection procedures collect similar data; however, the collection method varies depending on the source release. Only one of the following procedures is to be executed for the pre-upgrade data collection. Refer to Table 9 for guidance on which procedure to use.

If the Source Release is	Use This Pre-Upgrade Data Collection Procedure
8.0 and later	Procedure 4

 Table 9. Release Specific Data Collection Procedures

3.4.3.2 Data Collection for Source Release 8.0 and Later

This procedure collects and archives system status data for analysis. Perform this procedure only if the source release is 8.0 and later.

Procedure 4. Data Collection for Source Release 8.0 and Later

Step #	Procedure	Description					
	ocedure retrieves a off $()$ each step as	•		-			ider each step
f this pr	ocedure fails, it is	recommended	to contact My C	racle Suppo	ort (MOS) an	d ask fo	r assistance.
1.	Active NOAM VIP: Run the automated	-	to Administrat e active NOAM.	ion > Softw	are Manage	ment >	Upgrade.
	health checks on the active NOAM	Main Menu: Ad	dministration -> S	oftware Mana	gement -> Upg	rade	
		IPFE_SG MP_S					
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade 150
		NO1	Ready	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.8.1
			Norm	N/A	NO_DSR_VM	0.000	
		NO2	Ready	Standby	Network OAM&P	DAM&P	8.0.0.0.0-80.8.1
		10. If the ISO		ns section, a	select the Ad has already b	een per	Jpgrade optic
		Otherwise	e, do not select	an ISO.			
				anada aa	-		
		Control re	turns to the Up	grade scree	n.		

Step #	Procedure	Descripti	Description					
		Main Mer	nu: Administration	1 -> Softwar	e Managemen	t -> Upgrade Tue Apr 10 01:4!		
				OAM HA	Network Element	Application Version		
		NO1	Health Check	Role Standby	NE_NO	8.0.0.0.0-80.25.0		
		Health check	options					
		Checkup Type	Advance Upgrade Pre Upgrade Post Upgrade	Upgrade h	ealth check type.			
		Upgrade ISO	DSR-8.3.0.0.0_83.3.7-x86	64.iso v Select the	desired upgrade ISO medi	a file.		
2.	Active NOAM VIP: Monitor health check progress	Health Advar 2. Monitu The D 3. Click 4. Open	the Tasks option to on Check task name a inceUpgrade Health or the Health Check betails column displathe hyperlink to down the report and revie	Appears as <n Check. task until the T ys a hyperlink hload the Heal w the results. Management -> U Name No. 50 Advance()grade meatric Check Pre-upgrade full backup</n 	OServerGroup> ask State is cor to the Health Ch th Check report.	npleted. neck report.		
3.	Active NOAM VIP: Analyze any health check failure	Check log 1. Navig 2. Selec 3. Locate 4. Revie Analyze th	Ith Check report stat is can be analyzed to ate to Status & Mar t the UpgradeHealt e the log entries for t w the log for failures he failures and deter y, it is recommended	o determine if t hage > Files. hCheck.log file he most recer mine if it is saf	he upgrade can e and click View t health check. e to continue the	proceed. e upgrade. If		

Step #	Procedure	Description					
4.	Active NOAM VIP: Initiate SOAM health check	 Navigate Select the Select the Select the 		i on > Softv group tab.	vare Manage	ement > l	
		IPFE_SIG MP_S	Upgrade State	OAM HA Role	Server Role	Function	Application Version
		Hostname	Server Status	Appl HA Role	Network Element	Torney a	Upgrade ISO
		SOT	Ready	Active	System OAM	OAM	8.0.0.0.0-60.8.1
			Warm	NA	SO1_DSR_VM		
		902	Ready	Standby N/A	System OAM SO1_DSR_VM	OAM	8.0.0.0.0-80.8.1
			Norm	(NIC	SOT_DSM_VM		
		ISO optic 7. Click OK Control re	eturns to the Up	ct an ISO fo	r an increme en.	ntal upgra	
		\$01 H	Health Check		OAM HA Role Netv	vork Element	Application Version
					Active NE_	NO	8.0.0.0.0-80.25.0
			·				
			Advance Upgrade				
		Checkup Type	Pre Opgrade		Upgrade health cheo	k type.	
					Upgrade health chec Select the desired up		dia file.

Step #	Procedure	Description						
5. □	Active NOAM VIP: Monitor health check	 Click the Tasks option to display the currently executing tasks. The Health Check task name appears as <soservergroup> AdvanceUpgrade Health Check.</soservergroup> 						
	progress	 Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. 						
		3. Click the hyperlink to download the Health Check report.						
		4. Open the report and review the results.						
		Main Menu: Administration -> Software Management -> Upgrade						
		Filter" • Status • Taska" •						
		IPFE_9G MP_9G ID Hostname Name Task State Details Progress						
		Hostiname 2 ND1 BO_SG AdvanceUpgrade completedSO_SO_20100608-141156- Health CheckSO_20100608-141156- UTCbu						
		SO1 1 NO1 NO_SG AdvanceUpgrade completed AdvanceUpgrade HealthCheck NO_SG_201018059-140326*						
		802 D MP1 Pre-upgrade full backup completed Full backup on MP1 100%						
		 Select the active SOAM tab. Select the UpgradeHealthCheck.log file and click View. Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact My Oracle Support (MOS) for guidance. 						
7.	Analyze and plan MP upgrade sequence	 From the collected data, analyze system topology and plan for any DA-MP/IPFE/SBR/PCA which are out-of-service during the upgrade sequence. 1. Analyze system topology data gathered in Section 3.4.3.1 and steps 1. through 6. of this procedure. The Health Check reports from steps 3. and 6. can be found in Status & Manage > Files on the active SOAM. 2. It is recommended to plan for MP upgrades by consulting My Oracle Support (MOS) to assess the impact of out-of-service MP servers. 3. Determine the manner in which the MP servers are upgraded: Manually 						
		or Automated Server Group Upgrade. If the MPs are upgraded manually, determine the exact sequence in which MP servers are upgraded for each site.						

3.4.4 Back Up TKLCConfigData Files

This procedure helps to restore networking and server-related information in some cases. For example, disaster recovery when it needs to be performed on servers in case a server is lost during an upgrade.

Step #	Procedure	Description								
This pro	cedure backs up	the TKLCConfigData file on all servers.								
number.		s it is completed. Boxes have been provided for this purpose under each step recommended to contact My Oracle Support (MOS) and ask for assistance.								
1.	Active NOAM GUI: Login	Use the VIP address to access the primary NOAM GUI								
2.	Primary DSR NOAM VIP (GUI): Export	 Navigate to Configuration > Servers. Select each server in the topology and click Export. 								
	configuration	Main Menu: Configuration -> Servers								
	data for each	Configuration								
	server	Nativerta Hostsame Role System @ Server Group Hetwork Element Location								
		Roder E2B158ndFeatrOMI2 Interven DAMEP RODE RODER E2B1524005- E2B1524005- E2B1524005- E2B1524005- E2B1524005- E2B1524005-								
		Servers E2010ayd*va8x044/t Network D4464P NOSG Drdsg*va8x44_E201Gevent								
		Resource Domains E2R08indFeatS04M1 System 0441 00_50 BridingFeature_ 62830aext1 Places								
		Prace Associations E28(2BindFeatSOAN2 System OAN S0_00 BindingFeature, E282Genet2								
		a) D Nama & Events , E1811BnoFeatD4MP1 MP D4MP_SG BrodiniFeatUrit _ E1811								
		E1812SindFad885R1 MP B68R_00 BindesFedure_ E1812								
		Bisterer Bister Bister								
		Distances District E2050exdFeatSSER1 MP BOBRDS BridgeFeators E205 Processes								
		ja ⊡ Taana E2R/Bin/FratSSBR2 NP SSBR36 Bin/drgFrature, E2Bi D Fini ja SSBR36 S0482								
		12) Report Communication Apprix Desaulter Communication Apprix Desaulter Communication Apprix								
		4. Repeat this for all servers.								
3.	Primary SDS NOAM Server:	1. Access the primary DSR NOAM server command line using ssh or a console.								
	Back up TKLCConfig data	ssh admusr@ <noam vip=""></noam>								
		 Transfer the TKLCConfigData files for all servers in the /var/TKLC/db/filemgmt directory to a remote location. 								
		<pre>\$ cd /var/TKLC/db/filemgmt</pre>								
		\$ scp TKLCConfigData. <sever hostname="">.sh</sever>								
		<pre><username>@<remote-server>:<directory></directory></remote-server></username></pre>								
		Example:								
		<pre>scp TKLCConfigData.DSRN01.sh <username>@<remote- server>:<directory></directory></remote- </username></pre>								
		_								
		Remember to back up the TKLCConfig data file for all servers.								

3.4.5 Full Backup of DB Run Environment at Each Server

The procedures in this section are part of software upgrade preparation and are used to conduct a full backup of the run environment on each server, to be used in the event of a back out of the new software release. The backup procedure to be executed is dependent on the software release that is running on the active NOAM.

Note: Do not perform this procedure until the ISO deployment is completed to all servers in the topology. Failure to complete the ISO may disrupt ISO deployment/undeployment in the event of a partial backout (for example, backout of one site).



3.4.5.1 Full Backup of DB Run Environment for Release 8.0.x and Later

This procedure backs up the DB run environment when the active NOAM is on release 8.0.x and later.

Procedure 6. Full Backup of DB Run Environment for Release 8.0.x and Later

Step #	Procedure	Description					
	cedure (executed from server, so that each					ne run ei	nvironment
Check o number.	off ($ lap{d}$) each step as it i	s completed. B	oxes have bee	en provided f	for this purpo	ose unde	er each step
If this pr	ocedure fails, it is rec	ommended to c	ontact My Ora	cle Support	(MOS) and a	ask for a	ssistance.
1.	Active NOAM VIP: Start backup of all servers	 Navigate t Click Bac 	ministration -> S	ion > Softw	vare Manage	rade	Upgrade.
		Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
		The second second	Server Status	Appl HA Role	Network Element		Upgrade ISO
		NO2	Ready	Active	Network OAM&P	OAM&P	8.0.0.0.0-80.25.0
			Norm	N/A	NE_NO		
		NOT	Ready	Standby	Network OAM&P	OAM&P.	8.0.0.0.0-80.25.0
		*]					
		Backup Backup Al	Checkup Checku	p All Auto Upgrad	te Accept Repo	Report A	JII

Step #	Procedure	Description							
2.	Active NOAM VIP: Select network elements to backup	The Upgrade Backup All screen displays the various network elements and identifies which servers are ready for backup.							
		1. In the Action column, mark the Back up checkbox for each network element.							
		2. Ensure the I	E xclude op	otion is seled	cted.				
		3. Click OK.							
		This initiates Main Menu: Admin					Backup All] — Tue Apr 10 01:53:44 2018 EDT		
		Network element	Action	Server(s) in the pro	per state for backup	,	-		
		NE_NO	🛃 Back up	N01 801 N02 802					
		Full backup options							
		Database parts exclusion	 Exclude Do not exclude 	Select "Exclude" to perform a full backup of the COMCOL run environment, excluding the database parts specified in the files in Aust/TKLC/appworks/etc/exclude_parts d/ Select "Do not exclude" to perform a full backup of the COMCOL run environment without excluding any database parts. This will take longer and produce larger backup files in /var/TKLC/db/filemgmt.					
		Ok Cancel							
3.	Active NOAM VIP: Monitor	Select each serv Backup in Prog			/ each serv	er trans	sitions from		
	backup progress	Main Menu: Admi	nistration ->	• Software Ma	anagement -	> Upgrad	de		
		Fitar + Tana +							
		NO_SG IPFE_SG	MP_SG SO_SG						
		Hostname	Upgrade State Server Status	OAM Max HA Role Appl Max HA Role		Function	Application Version Upgrade ISO		
		NO1	Backup In Progress Norm	Active N/A	Network OAM&P NO_DSR_VM	OAMAP	7.1.1.0.0-71.31.0		
		N02	Backup In Progress Norm	Standby N/A	Network OAM&P NO_DSR_VM	CAMEP	7.1.1.0.0-71.31.0		
		Backup Backup All	Auto Upgrade	Accept Report	Report All				

Step #	Procedure	Description
4.	ALTERNATIVE METHOD (Optional) Server CLI: If needed, the alternative backup method can be executed on each individual server instead of using the backupAllHosts script	ALTERNATIVE: A manual backup can be executed on each server individually, rather than using the GUI method. To do this, log into each server in the site individually, and execute this command to generate a full back up on that server manually: \$ sudo /usr/TKLC/appworks/sbin/full_backup Output similar to the following indicates successful completion: Success: Full backup of COMCOL run env has completed. Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullDBParts. SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt. Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullRunEnv. SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullRunEnv. SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.
5.	Active NOAM VIP: Verify backup files are present on each server	 Log into the active NOAM. Navigate to Status & Manage > Files. Click on each server tab. For each server, verify the following 2 files have been created: Backup.DSR.<server_name>.FullDBParts.NETWORK_OAMP.<t ime_stamp>.UPG.tar.bz2 Backup.DSR.<server_name>.FullRunEnv.NETWORK_OAMP.<ti me_stamp>.UPG.tar.bz2</ti </server_name></t </server_name>

3.4.6 IDIH Pre-Upgrade

If IDIH is a component of a Network Element, it should be upgraded only after the DSR. However, it should be noted that certain compatibility limitations may exist while the two components (DSR and IDIH) are not on the compatible release.

The IDIH upgrade procedures are provided in Appendix E and may be performed at any time after Section 3.4.6.1 has been completed.

Table 10. IDIH Upgrade Preparation Overview

	Elapsed Time (hr:min)		
Procedure	This Step	Cum.	Procedure Title
Procedure 7	0:15-0:30	0:15-0:30	Procedure 7

3.4.6.1 IDIH Upgrade Preparation

Procedure 7. IDIH Upgrade Preparation

Step #	Procedure	Description							
	This procedure prepares the Mediation and Application guests for upgrade. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.								
If this proc	cedure fails, it is re	commended to contact My Oracle Support (MOS) and ask for assistance.							
1. Place the Mediation and Application OVAs in the cloud repository Follow the hypervisor's instructions to add the Mediation and Application OVAs to the cloud repository.									

3.5 Software Upgrade Execution Overview

It is recommended to contact My Oracle Support (MOS) before executing this upgrade to ensure that the proper media are available for use.

Before upgrading, users must perform data collection and system health check procedures in section 3.4. This ensures the system to be upgraded is in an upgrade-ready state. Performing the system health check determines which alarms are present in the system and if an upgrade can proceed with alarms.



If there are servers in the system which are not in a Normal state, these servers should be brought to the Normal or Application Disabled state before the upgrade process is started. The sequence of upgrade is such that servers providing support services to other servers are upgraded first.

If alarms are present on the server, it is recommended to contact My Oracle Support (MOS) to diagnose those alarms and determine whether they need to be addressed, or if it is safe to proceed with the upgrade.

Please read the following notes on upgrade procedures:

- All procedure completion times shown in this document are estimates. Times may vary due to differences in database size, user experience, and user preparation.
- The shaded area within response steps must be verified in order to successfully complete that step.
- Where possible, command response outputs are shown as accurately as possible. EXCEPTIONS are as follows:
 - Session banner information such as time and date.
 - System-specific configuration information such as hardware locations, IP addresses and hostnames.
 - ANY information marked with XXXX or YYYY. Where appropriate, instructions are provided to determine what output should be expected in place of XXXX or YYYY.
 - Aesthetic differences unrelated to functionality such as **browser attributes: window size**, **colors**, **toolbars**, and **button layouts**.

- After completing each step, and at each point where data is recorded from the screen, the technician performing the upgrade must initial each step. A checkbox is provided. For procedures which are executed multiple times, the checkbox can be skipped, but the technician must initial each iteration the step is executed. The space on either side of the step number can be used (margin on left side or column on right side).
- Captured data is required for future support reference if a representative is not present during the upgrade.
- Answer these questions, and record:

What is the DSR Application version to be upgraded?						
What is the DSR Application new version to be applied?						
Is this a Major or Incremental Upgrade?						
Are there IPFE servers to upgrade?						
Is SDS also deployed (co-located) at the DSR site?						
<i>Note</i> : SDS does not need to be upgraded at the same time.						
Is IDIH also deployed (co-located) at the DSR site?						

3.5.1 Accepting the Upgrade

After the upgrade of ALL Servers in the topology has been completed, and following an appropriate soak time, the Post-Upgrade procedures in Section 5.4 are performed in a separate Maintenance Window to finalize the upgrade. Procedure 40 accepts the upgrade and performs a final Health Check of the system to monitor alarms and server status. Accepting the upgrade is the last step in the upgrade. Once the upgrade is accepted, the upgrade is final and cannot be backed out.

4. NOAM Upgrade Execution

NOAM UPGRADE

The NOAM upgrade section is common to all topologies. This section must be completed before executing the site upgrade procedures.

Procedures for the NOAM upgrade include steps for the upgrade of the Disaster Recovery NOAM (DR NOAM) servers also. If no DR NOAM is present in the customer deployment, then the DR NOAM-related steps can be safely ignored.

Global Provisioning is disabled before upgrading the NOAM servers. Provisioning activities at the NOAM and SOAM servers have certain limitations during the period where the NOAMs are upgraded and the sites are not yet upgraded.

The Elapsed Time mentioned in Table 11 specifies the time to upgrade the DSR application. All times are estimates.

	Elapsed Tir	ne (hr:min)			
Procedure	This Step Cum.		Procedure Title	Impact	
Procedure 8	0:20-0:30	0:20-0:30	Procedure 8	None	

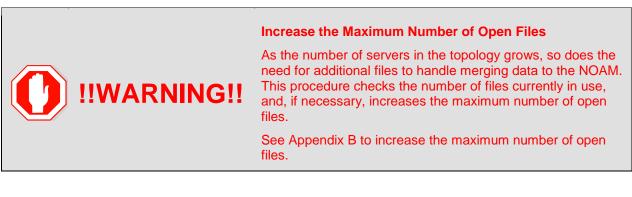
Table 11. NOAM Upgrade Execution Overview

	Elapsed Time (hr:min)			
Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 9	0:05-0:10	0:25-0:55	Procedure 9	None
Procedure 10	0:01-0:05	0:26-1:00	Procedure 10	Global Provisioning Disabled
Procedure 11	0:40-1:20	1:06-2:20	Procedure 11	No Traffic Impact
Procedure 12	0:06-0:20	1:12-2:40	Procedure 12	None
Procedure 13	Procedure 13 0:05-0:10 1:17-2:50		Procedure 13	Global Provisioning Enabled

4.1 NOAM Pre-Upgrade Checks and Backup

The procedures in this section perform health checks and backups to prepare the NOAM NE for upgrade. These procedures must be executed on the active NOAM.

- *Note*: These procedures may be executed outside of the maintenance window, but should be executed within 6 to 8 hours before Procedure 11.
- *Note*: If syscheck fails on any server during pre-upgrade checks or in early checks stating that **cpu: FAILURE:** No record in alarm table for **FAILURE!**, see Procedure 68.



4.1.1 NOAM Health Check for Source Release 8.0 and Later

This procedure is used to determine the health and status of the network and servers when the NOAM is on source release 8.0 or later. This procedure must be executed on the active NOAM.

Procedure 8. NOAM Health Check for Source Release 8.0 or Later

Step #	Procedure	De	scription							
This pro	cedure performs a	l Hea	alth Check of the system before upgrading the NOAMs.							
Check o number.		it is	completed. Boxes have been provided for this purpose under each step							
If this pr	f this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.									
1.	Active NOAM	5.	Navigate to Status & Manage > Files.							
	VIP: Verify upgrade DSR ISO has been	6.	Select the target release DSR ISO and click View ISO Deployment Report.							
	transferred to all servers	7.	Review the report to ensure the ISO is deployed to all servers in the topology.							
			Sample report:							
			Deployment report for DSR-DSR-8.6.0.0.0_95.14.0- x86_64.iso:							
			Deployed on 7/7 servers.							
			NO1: Deployed							
			NO2: Deployed							
			SO1: Deployed							
			SO2: Deployed							
			MP1: Deployed							
			MP2: Deployed							
			IPFE: Deployed							
2.	Active NOAM	1.	Navigate to Diameter Common > Export.							
	VIP: Export and archive the Diameter configuration data	2.	Capture and archive the Diameter data by selecting the ALL option for the Export Application.							
		3.	Verify the requested data is exported by clicking Tasks at the top of the screen.							
		4.	Navigate to Status & Manage > Files and download all the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.							

Step #	Procedure	Descriptio	on							
3.	Active NOAM VIP: Initiate NOAM health checks	 This procedure runs the automated pre-upgrade health checks. 1. Navigate to Administration > Software Management > Upgrade. 2. Select the active NOAM. Main Menu: Administration -> Software Management -> Upgrade								
			Filter* • Tosks* •							
		IPFE_SG I	MP_SG NO_SG SO_SG Upgrade State Server Status	OAM HA Role	Server Role Network Element	Function	Application Version Upgrade 150			
		NO1	Ready	Active	Network OAM&P	OAM&P	8.0.0.0.0-60.8.1			
		NO2	Ready Norm	N/A Standby N/A	NO_DSR_VM Network OAM&P NO_DSR_VM	OAM&P	8.0.0.0.0-80.8.1			
		3. Click C 4. Under	Checkup Checkup Checkup Checkup. Health Check opti he Upgrade ISO o	ons, select th	ne Pre Upgr		ion.			
		0.485 0.000	DK. I returns to the Up Iministration -> Software	N 11 1 1		1				
		latat a		nunuyement > u	pyruue [encour	-1				
		Rochame	Action	Mahan						
		N18-80-63	Health Check	GAM IN	A Role Betwork Dem ISX_NDAB_NE		Application Version 0.2111-0251			
		Health check options Checkou Tape	Advance Uppelle @ Pre Uppelle	Upgrafe	wallh sherik type.					
		Augrade 190	C Paul Uppradu bygrade 100 DSP-6.2.0.0.0_82.6.1.406_64 km							
		204 Carrott								

Step #	Procedure	Description							
4. □	Active NOAM VIP: Monitor health check progress for completion	 Click the Tasks option to display the currently executing tasks. The Health Check task name appears as <noservergroup> PreUpgrade Health Check.</noservergroup> 							
		2. Monitor the Health Check task until the Task State is completed.							
			•	lays a hyperlinl wnload the Hea		e Health Check re eck report.	eport.		
		4. Open the report and review the results.							
		Main Menu: Admin	nistration -> Softwa	are Management ->	Upgrade	(_	
		Filter* • Status •	Tasks* -						
		IPFE_80 MP_90	Tasks ID Hostname	Name	Task State	Defails	Progress		
		Hostsame	1 NO1	NO_SO AdvanceUpgrade Health Check	completed	AdvanceUpgrade_HearthCheck _NO_SG_20160808-140326- UTC.bt	500%		
		NO1	D MP2	Pre-upgrade full backup	completed	Full backup on MP2	100%		
		N02	0 MP1	Pre-upgrade full backup Pre-upgrade full backup	completed	Full backup on IPFE1 Full backup on MP1	100%	~	
5.	Active NOAM VIP: Analyze health check results	 Analyze health check report for failures. If the Health Check report status is anything other than Pass, analyze the Health Check logs to determine if the upgrade can proceed. 1. Navigate to Status & Manage > Files. 2. Select the AdvancedUpgrade_HealthCheck_<noam sg="">_<timestmp>.txt file and click View.</timestmp></noam> 3. Locate the log entries for the most recent health check. 4. Review the log for failures. 5. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact My Oracle Support (MOS). 				he			

4.1.2 NOAM Pre-Upgrade Backup

This procedure takes a backup of the NOAM servers just prior to the upgrade.

Procedure 9. NOAM Pre-Upgrade Backup

Step #	Procedure	De	scriptio	n				
This pro	This procedure takes a backup of the NOAM.							
number.			•	ted. Boxes have been provided for this purpose under each step				
	this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.							
1.	Active NOAM VIP: Backup	6.	•	ate to Status & Manage > Database to return to the Database screen.				
	all global configuration	7.	Click to	b highlight the active NOAM server and click Backup .				
	databases for		Note:	Backup is only enabled when the active server is selected.				
	NOAM	8.	Mark t	he Configuration checkbox.				
	<i>Important</i> : Required for disaster recovery	9.		the desired compression type. Retain the default selection unless s a specific reason or direction to change it.				
		10.	Enter (Comments (optional).				
		11.	Click C	DK.				
			Note:	On the Status & Manage >Database screen, the active NOAM server displays the word Active in the OAM Max HA Role column.				
2. Active NOAM		1.	Naviga	ate to Status & Manage > Files .				
	VIP: Download/Save database files backups for NOAM	2.	Click o	n the active NOAM server tab.				
		3.	Select	the configuration database backup file and click Download .				
		4.	If a cor	nfirmation window displays, click Save .				
	<i>Important</i> : Required for	5.		Choose File screen displays, select a destination folder on the local ation to store the backup file. Click Save .				
	disaster recovery	6.	lf a Do	wnload Complete confirmation displays, click Close .				

4.2 Disable Global Provisioning

The following procedure disables provisioning on the NOAM. This step ensures no changes are made to the database while the NOAMs are upgraded. Provisioning is re-enabled once the NOAM upgrade is complete.

Procedure 10. Disable Global Provisioning

Step #	Procedure	Description					
This pro	This procedure disables provisioning for the NOAM servers.						
number.	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.						
1.	Active NOAM	1. Log into the active NOAM GUI using the VIP.					
	UIP: Disable global	2. Navigate to Status & Manage > Database.					
	provisioning	3. Click Disable Provisioning.					
	and configuration	4. Confirm the operation by clicking OK on the screen.					
	updates on the entire network	 Verify the button text changes to Enable Provisioning; a yellow information box should also display at the top of the view screen that states: 					
		[Warning Code 002] – Global provisioning has been manually disabled.					
		The active NOAM server has the following expected alarm:					
		Alarm ID = 10008 (Provisioning Manually Disabled)					

4.3 NOAM Upgrade

This procedure is used to upgrade the NOAM and DR NOAM servers.

Procedure 11. NOAM Upgrade

Step #	Procedure	Description			
		ne NOAM servers. it is completed. Boxes have been provided for this purpose under each step			
If this pr	ocedure fails, it is r	ecommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	Upgrade primary DSR standby NOAM	 Upgrade the primary DSR standby NOAM server using Upgrade Single Server procedure: If the active NOAM is on DSR 8.x: Execute Appendix C Upgrade Single Server – DSR 8.x. Otherwise: Execute Error! Reference source not found Error! Reference so urce not found After successfully completing the procedure in Appendix C or Error! Reference source not found., return to this point and continue with the next step. The active NOAM server may have some or all of the following expected alarms: Alarm ID = 10008 (Provisioning Manually Disabled) Alarm ID = 10073 (Server Group Max Allowed HA Role Warning) Alarm ID = 31101 (DB Replication to slave DB has failed) Alarm ID = 31107 (DB Merge to Parent Failure) Alarm ID = 31225 (HA Service Start Failure) Alarm ID = 31233 (HA Path Down) Alarm ID = 32532 (Server Upgrade Pending Accept/Reject) Alarm ID = 31114 (DB Replication over SOAP has failed) If the upgrade fails – do not proceed. It is recommended to consult with on the best course of action. 			
2.	Upgrade second DSR NOAM	Upgrade the second DSR NOAM server using the Upgrade Single Server procedure: Execute Appendix C Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and continue with the next step.			
3.	Upgrade standby DR NOAM	Upgrade the standby DR NOAM server using the Upgrade Single Server procedure: Execute Appendix C Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and continue with the next step.			

Step #	Procedure	Description
4.	Upgrade active DR NOAM	Upgrade the active DR NOAM server using the Upgrade Single Server procedure: Execute Appendix C Upgrade Single Server – DSR 8.x.
		After successfully completing the procedure in Appendix C, return to this point and continue with the next procedure per Table 11.

4.4 Verify NOAM Post Upgrade Status

This procedure determines the validity of the upgrade, and the health and status of the network and servers.

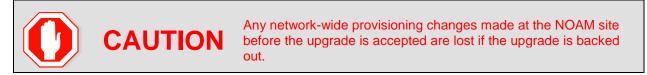
Procedure 12	Verify NOAM Post Upgrade Status
--------------	---------------------------------

Step #	Procedure	Description				
Check c number.		it is completed.	Boxes have	e been pro		rpose under each step d ask for assistance.
1.	Active NOAM VIP: Post- upgrade health checks	 Navigate to Select the a Main Menu: Admi Filter Tasks * 	o Administr a active NOAM	ation > So	ost-upgrade hea oftware Manage gement -> Upgrade Server Role Funct Network Element	ment > Upgrade.
		NOT	Accept or Reject	Active	Network GAMEP GAME NO_DER_VM	P 80000-809.0 DSR-6.0.0.0.0.90-86_64.iso
		5. Click OK .	Accept or Reject Warn Checkup Checkup	Standby NA All Opproducto tions, sele	Network OAMAP CAMA NO_DSR_VM	P 8.0.0.00-80.9.0

Step #	Procedure	Description					
		Main Menu: Administration -> Software Management -> Upgrade [Checkup]					
		Hostname Action Status					
		NO1 Health Check OAM HA Role Network Element NO_DSR_VM					
		Health check options					
		Checkup Type Pie Upgrade Upgrade Health check type.					
		Upgrade ISO - Select - Select The desired upgrade ISO media file.					
		Ok Cancel					
2.	Active NOAM VIP: Monitor health check progress	 Click the Tasks option to display the currently executing tasks. The Health Check task name appears as <noservergroup> PostUpgrade Health Check.</noservergroup> Monitor the health check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. Click the hyperlink to download the Health Check report. Click the hyperlink to download the Health Check report. Open the report and review the results. Main Menu: Administration > Software Management > Upgrade Image: Tasks of the Management > Upgrade					
3.	Active NOAM VIP: Analyze health check failures	 If the Health Check report status is anything other than Pass, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Navigate to Status & Manage > Files. 2. Select the file named UpgradeHealthCheck.log and click View. 3. Locate the log entries for the most recent health check. 4. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact My Oracle Support (MOS) for guidance. 					

4.5 Allow Provisioning (Post NOAM Upgrade)

The following procedure enables Global Provisioning after the NOAM upgrade.



Procedure 13. Allow Provisioning (Post NOAM Upgrade)

Step #	Procedure	Description						
This pro	This procedure enables provisioning for the NOAM and DR NOAM servers.							
Check c number.	()	it is completed. Boxes have been provided for this purpose under each step						
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.						
1.	Active NOAM	1. Log into the active NOAM GUI using the VIP.						
	VIP: Enable global	2. Navigate to Status & Manage > Database.						
	provisioning	3. Click Enable Provisioning.						
	and configuration	4. Confirm the operation by clicking OK on the screen.						
	updates on the entire network	5. Verify the button text changes to Disable Provisioning.						
	Note : After enabling provisioning at the NOAM, the SOAM GUI(s) may display a banner indicating that global provisioning is disabled. This message can be ignored – global provisioning is enabled. This is a display issue only and is corrected when the SOAMs are upgraded.							
2.	Active NOAM VIP: Add new	Perform this step only if the addition of a new network element is required at this time.						
	network element (if required)	If a new network element is to be added, start this procedure now. The addition of the new network element requires a separate maintenance window. The servers in the new network element must be installed with the same DSR release as that of the upgraded NOAM(s). Follow the release specific installation procedures from reference [1] to install the software on the new servers and add the new network element under the existing NOAM(s). Skip the sections of the installation procedure related to installing and configuring the NOAM(s). This adds a new DSR SOAM site under the existing NOAM(s).						

5. Site Upgrade Execution

This section contains the procedures for upgrading an entire site - starting with the pre-upgrade activities, upgrading the SOAMs and C-level servers, and finishing with verifying the upgrade.

To maximize the Maintenance Window usage, the procedures in this section make full use of the parallel upgrade capabilities of the DSR, while ensuring traffic continuity and redundancy to the fullest extent possible.

CAUTION Read 2.4 Automated Site Upgrade for details and limitations/solutions while doing planning of upgrade cycles.

The Automated Site Upgrade procedures are in section 5.2: Automated Site Upgrade. Use the procedures in this section if the Automated Site Upgrade was recommended in section 3.3 Site Upgrade Methodology Selection. See section 5.2.3 for more details for rearranging cycles, if needed.

The manual site upgrade procedures are in section 5.3. Use the procedures in this section if the manual upgrade was recommended in section 3.3 Site Upgrade Methodology Selection.

5.1 Site Pre-Upgrade Activities

SITE UPGRADE: Pre-Upgrade Activities

Use this section to execute pre-upgrade planning, pre-upgrade backups, pre-upgrade health checks, and to disable site provisioning.

This section contains the procedures for site upgrade planning, pre-upgrade backups, health checks, and disabling site provisioning.

Table 12 shows the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use Table 12 as a guide for determining the order in which the procedures are to be executed.

	Elapsed Time (hr:min)		psed Time (hr:min)	
Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 14	0:10-0:20	0:10-0:20	Procedure 14 Site Pre-Upgrade Backups	None
Procedure 15	0:05-0:10	0:15-0:30	Procedure 15 Site Pre-Upgrade Health Check for Release 8.0 and Later	None None
Procedure 16	0:03	0:18-0:38	Procedure 16 Site Upgrade Options Check	None
Procedure 17	0:01-0:05	0:19-0:48	Procedure 17 Disable Site Provisioning	Site Provisioning Disabled, No Traffic Impact
Procedure 18	0:05-0:10	0:24-0:58	Procedure 18 Site Upgrade Pre-Checks	None

Table 12.	Site Upgrade	Execution	Overview
-----------	--------------	-----------	----------

	Elapsed Time (hr:min)		Elapsed Time (hr:min)		
Procedure	This Step	Cum.	Procedure Title	Impact	
Procedure 19	2:40-4:00	3:04-4:58	Procedure 19 Automated Site Upgrade	Traffic is not serviced by servers that are actively upgrading.	
Procedure 20	0:02	3:06-5:00	Procedure 20 Rearrangement of upgrade cycles for Automated Site Upgrade	Site Provisioning Enabled, No Traffic Impact	
Procedure 21	0:10-0:15	3:26-5:15	Procedure 21 SOAM Upgrade Pre-Checks	None	

5.1.1 Site Pre-Upgrade Backups

This procedure is non-intrusive and is used to perform a backup of all servers associated with the SOAM Site(s) being upgraded. It is recommended that this procedure be executed no earlier than 36 hours prior to the start of the upgrade.

Since this backup is to be used in the event of disaster recovery, any site configuration changes made after this backup should be recorded and re-entered after the disaster recovery.

Procedure 14 is an alternate procedure that can be used to backup a site using the command line. Procedure 14 should only be used by direction of My Oracle Support (MOS).

Procedure 14. Site Pre-Upgrade Backups

Step #	Procedure	Description				
	This procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary.					
Check o number.		as it is completed. Boxes have been provided for this purpose under each step				
If this pr	ocedure fails, it is	s recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	Active SOAM	1. Log into the SOAM GUI using the VIP.				
	VIP: Back up site configuration	 Navigate to Status & Manage > Database to return to the Database Status screen. 				
	data	3. Click to highlight the Active SOAM server, and click Backup.				
	<i>Important</i> : Required for	<i>Note</i> : Backup is only enabled when the active server is selected.				
	disaster	4. Mark the Configuration checkbox.				
	recovery	5. Select the desired compression type. Retain the default selection unless there is a specific reason or direction to change it.				
		6. Enter Comments (optional).				
	7. Click OK .					
		 Note: The active SOAM can be determined by navigating to Status & Manage > HA and noting which server is currently assigned the VIP in the Active VIPs field. The server having VIP assigned is the Active. 				

Step #	Procedure	Description					
2.	Active SOAM VIP: Download/Sav e database backup files <i>Important</i> . Required for disaster recovery	 Navigate to Status & Manage > Files. Click on the active SOAM server tab. Select the configuration database backup file and click Download. If a confirmation window displays, click Save. If the Choose File window displays, select a destination folder on the local workstation to store the backup file. Click Save. If a download complete confirmation displays, click Close. 					
3.	Active NOAM VIP: Upgrade/Back up DB run environment for site	 Log into the NOAM GUI using the VIP. Navigate to Administration > Software Management > Upgrade. Click Backup All. Main Menu: Administration -> Software Management -> Upgrade Filler* Tasks * PFE SG MP. SG NO SG SO SG					
		Hostname Upgrade State OAM HA Role Server Role Function Application Version NO1 Server Status Appl HA Role Network CAM&P OAM&P 8.0.0.0-90.9.0 NO1 Accept or Reject Active Network OAM&P OAM&P 8.0.0.0-90.9.0 NO1 Warn N/A NO_DSR_VM DSR-8.0.0.0.9.0.9.0 NO2 Accept or Reject Standby Network OAM&P OAM&P 8.0.0.0-90.9.0 NO2 Accept or Reject Standby Network OAM&P OAM&P 8.0.0.0-90.9.0 NO2 Accept or Reject Standby Network OAM&P OAM&P 8.0.0.0-90.9.0 NO2 Backup All Checkup All Auto Upgrade Accept Report All					

Step #	Procedure	Description	Description					
4.	Active NOAM VIP: Set backup parameters	 The Upgrade Backup All screen displays the various network elements a identifies which servers are ready for backup. 1. In the Action column, mark the Back up checkbox for each network element. 2. Verify the NOAM server group checkbox is NOT marked. <i>Note</i>: Backing up the NOAM servers at this point overwrites the pre-upgrade backup files needed for backing out the target release. Do NOT back up the NOAM servers. 3. In the Full Backup Options section, verify the Exclude option is sele 4. Click OK. This initiates a full backup on each eligible server. 				h network ites the he target ion is selected.		
		Network element	Action	Server(s) in the proper s	state for backup			
		NO_DSR_VM	None					
		SO1_DSR_VM	V Back up	SO1 SO2 MP1 MP2 IPF	E1			
		Full backup options						
		Database parts exclusion Ok Cancel	 Exclude Do not exclude 	Select "Exclude" to perfor in /usr/TKLC/appworks/etr Select "Do not exclude" to and produce larger backu	c/exclude_parts.d/.	he COMCOL run enviror		
5. 🗌	Active NOAM VIP: Monitor tasks for backup completion	in step 4 are c	ogress of the omplete.	e backups until th	ne network elem	ient(s) selected		
	completion	Main Menu: Administ	ration -> Softw	are Management ->	Upgrade			
		Filter" (Tasks" -) Taska						
		IPFE_SG ID Hostn 2 902		Task State	Details Full backup on SO2	Progress		
		Hostname 10 MP2		ade full backup completed ade full backup completed	Full backup on SO2	100%		
		NO1 10 SO1		ade full backup completed	Full backup on SO1	100%		
		15 MP1	Pre-upor:	ade full backup completed	Full backup on MP1	100%		
		10 MP-1				~		

Step #	Procedure	Description		
6.	Active NOAM	1.	Log into the active NOAM or SOAM GUI.	
	VIP: Verify backup files	2.	Navigate to Status & Manage > Files.	
	are present on 3.		Click on each server tab.	
	each server.	4.	For each server, verify the following 2 files have been created:	
			Backup.DSR. <server_name>.FullDBParts.NETWORK_OAMP.<time _stamp>.UPG.tar.bz2</time </server_name>	
			Backup.DSR. <server_name>.FullRunEnv.NETWORK_OAMP.<time_ stamp>.UPG.tar.bz2</time_ </server_name>	
		5.	Repeat sub-steps 1 through 4 for each site being upgraded.	

5.1.2 Site Pre-Upgrade Health Checks

This section provides procedures to verify the health of the SOAM site prior to upgrade. Procedure 15 is the primary procedure to be executed when the active NOAM is on release 8.0 and later. Alternate release-specific procedures are also provided, to be used as directed.

5.1.2.1 Site Pre-Upgrade Health Check for Release 8.0 and Later

This procedure is used when the NOAMs are on release 8.0 and later. The procedure is non-intrusive and performs a health check of the site prior to upgrading.

Note: If syscheck fails on any server during pre-upgrade checks or in early checks stating that **cpu: FAILURE::** No record in alarm table for **FAILURE!**, see Procedure 68 Workaround to Resolve syscheck Error for CPU Failure.

Step #	Procedure	Description					
•	cedure performs a ff $()$ each step as			•		irpose u	nder each step
If this pr	ocedure fails, it is	recommended to	contact My C	racle Supp	ort (MOS) ar	nd ask fo	or assistance.
1.	1. Active NOAM VIP: Run site health checks (part 1)	 Select the ta Select the S 	Administrat ab of the site COAM server ctive SOAM. cup.	ion > Softw to be upgra group link.	gement -> Upg		
		NO_SG SO_East	SO_North SO_Wes		/1		
		Entire Site 50 East	IPFE1_SG IPFE2	_SG IPFE3_SG	IPFE4_SG MP_S	G SBR_SG	East
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
		801	Ready	Standby N/A	System OAM SO1_DSR_VM	DAM	7.2.0.0.0-72.25.0
		S02	Ready Norm	Active	System OAM SO1_DSR_VM	OAM	7.2.0.00-72.25.0
		SO2 Backup Backup All (N/A	SO1_DSR_VM	OAM port Report	

Procedure 15. Site Pre-Upgrade Health Check for Release 8.0 and Later

Step #	Procedure	Description					
2.	Active NOAM VIP: Run site health checks (part 2)	 Use the Upgr Click OK to in 	i p . check options s r ade ISO optior nitiate the health ns to the Upgrad	n to select the h check. de Administra	e target relea ation screen.	se ISO.	
		NO1 Health Ch	eck	OAM HA Role Standby	Network Element	Application Versio 8.0.0.0.0-80.25.0	on Version SO 30.25.0
		Health check options Advance Checkup Type Pre Upp Post Up Upprade ISO	irade	Upgrade health Select the desir Ok Cancel	check type. red upgrade ISO media	t file.	10.25.0
3.	Active SOAM VIP: Monitor health check progress for completion	Health Check Health Check Health Check Comment Health Check Check Health Check Check Health Check Health Check Check Health Check Check Health Check Check Check Health Check	lealth Check tas olumn displays erlink to downlo ort and review t ation -> Software Ma ation -> Software Ma	sk until the T a hyperlink to ad the Healt the results. Inagement -> Upg the results in agement -> Upg the results sever Upgrade corr	DServerGrou ask State is o to the Health h Check repo	Completed. Check report ort.	ade

Step #	Procedure	Description
4.	Active SOAM VIP: Analyze any health check failures	If the Health Check report status is anything other than Pass , the Health Check logs must be analyzed to determine if the upgrade can proceed. The Health Check log is located in the File Management area of the active SOAM. Select the active SOAM tab to see the Health Check log. 1. Navigate to Status & Manage > Files .
		 Navigate to Status & Manage > Thes. Select the active SOAM tab.
		 Select the UpgradeHealthCheck.log file and click View.
		 Locate the log entries for the most recent health check.
		 Review the log for failures.
		Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact My Oracle Support (MOS) for guidance.
		If the health check log contains the Unable to execute Health Check on <active hostname="" soam=""></active> message, perform an alternate health check procedure as follows:
		If the active SOAM release is 8.0/8.1:
		Execute SOAM Upgrade Pre-Checks.
5.	Active SOAM	1. Navigate to Diameter Common > Export .
	VIP: Export and archive the Diameter	 Capture and archive the Diameter data by selecting the ALL option for the Export Application.
	configuration	3. Click OK .
	data on active SOAM GUI	4. Verify the requested data is exported by clicking Tasks at the top of the screen.
		 Click File Management to view the files available for download. Download all of the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine.
6.	Capture data for each SOAM site	Repeat this procedure for each configured SOAM site to be upgraded.

5.1.3 Site Upgrade Options Check

Automated Site Upgrade provides user-configurable options that control certain upgrade behaviors. These options are found on the active NOAM's **Administration > General Options** screen and are described in detail in Section 2.4.3. Before initiating a site upgrade, review these options to verify the current settings are correct, or to modify the settings to meet customer requirements/preferences.

This procedure is applicable only to Auto Site Upgrade. The options have no effect on manual upgrades or Automated Server Group upgrades.

Procedure 16.	Site Upgrade Options Check
---------------	----------------------------

Step #	Procedure	De	Description		
 This procedure is used to review the site upgrade options and make changes as necessary. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance. 					
1.	Active NOAM VIP: View auto site upgrade options	 1. 2. 3. 4. 5. 6. 	Log into the active NOAM GUI. Navigate to Administration > General Options. Scroll down to the Site Upgrade Bulk Availability option. Review the existing value of this option and determine if changes are needed. If the option is changed, click OK to save the change. Scroll down to the Site Upgrade SOAM Method option. Review the existing value of this option and determine if changes are needed. If the option is changed, click OK to save the change.		

5.1.4 Disable Site Provisioning

This procedure disables Site Provisioning in preparation for upgrading the site.



This procedure may only be performed in the maintenance window immediately before the start of the SOAM site upgrade.

Procedure 17. Disable Site Provisioning

Step #	Procedure	Description			
 This procedure disables provisioning for the SOAM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance. 					
1.	Active SOAM VIP: Disable site provisioning	 Log into the SOAM GUI of the site to be upgraded. Navigate to Status & Manage > Database. Click Disable Provisioning. Confirm the operation by clicking OK on the screen. Verify the button text changes to Enable Provisioning. A yellow information box also displays at the top of the view screen that states: [Warning Code 004] – Site provisioning has been manually disabled. The active SOAM server has the following expected alarm: Alarm ID = 10008 (Provisioning Manually Disabled) 			
2.	Repeat for each SOAM site	Repeat this procedure for each configured SOAM site to be upgraded.			

5.2 Automated Site Upgrade



5.2.1 Site Upgrade Pre-Checks

This procedure verifies that the system is prepared for Automated Site Upgrade.

Procedui	Procedure 18. Site Upgrade Pre-Checks									
Step #	Procedure	Description								
	cedure verifies the site.	raffic status, and verifies that Site Provisioning is disabled, in preparation for								
Check o number.		as it is completed. Boxes have been provided for this purpose under each step								
If this pr	ocedure fails, it i	s recommended to contact My Oracle Support (MOS) and ask for assistance.								
1.	Active	1. Log into the active SOAM GUI using the VIP.								
	SOAM VIP: View KPIs to	2. Navigate to Status & Manage > KPIs.								
	View KPIs to verify traffic status	3. Inspect KPI reports to verify traffic is at the expected condition.								
2.	Active	Verify that Site Provisioning was properly disabled in Procedure 17.								
	SOAM VIP: Verify Site	In the GUI status bar, where it says Connected using , check for the message Site Provisioning disabled .								
	Provisioning is disabled	If the message is present, continue with the next procedure per Table 12; otherwise, execute Procedure 17.								

Procedure 18. Site Upgrade Pre-Checks

5.2.2 Initiate Automated Site Upgrade

This procedure initiates the Automated Site Upgrade sequence.

Procedure 19. Automated Site Upgrade

Step #	Procedure	Description
Check o number.	ff $()$ each step	s an entire site using the Automated Site Upgrade option. as it is completed. Boxes have been provided for this purpose under each step is recommended to contact My Oracle Support (MOS) and ask for assistance.
 1. □	Review site upgrade plan and site readiness	Review the site upgrade plan created in Section 3.2. This step verifies that the servers and server groups to be upgraded are in the proper state. 1. Log into the NOAM GUI using the VIP. 2. Select Administration > Software Management > Upgrade. 3. Select the SOAM tab of the site to be upgraded. 4. Verify the Entire Site link is selected. The Entire Site screen provides a summary of the server states and upgrade readiness. More detailed server status is available by selecting a specific server group link. Note: The Site Upgrade option can be used to upgrade an entire site, or a subset of site elements. The servers within the site may be in various states of readiness, including Accept or Reject, Ready, Backup Needed, Failed, or Not Ready. Only the servers in the Ready or Failed state are upgrade eligible.
2.	Active NOAM VIP: Initiate site upgrade	 Verify no server groups are selected on the upgrade administration screen. The Site Upgrade button is not available if a server group is selected. Click Site Upgrade. Review the upgrade plan as presented on the Site Initiate screen.

Procedure [Desci	ription									
	D	his plan repre ue to the dyr vel) may be	amic nature	of the upg	rade, som	e servers	s (typically				
	Main Menu: Administration -> Software Management -> Upgrade [Site Initiate]										
	1007										
	Cycle	Action	Servera								
	4)	lograde	CARGE AND CARGO AND	level u/SRJ000CAMOE - thin the	Function COPP (administrative paint)	Noticed Version OVM (Sure 228534	12.9.8				
	,	Vyng wite	SHARD_SSTHP_RG_	Server DASSAUBUTEUS - KITM DASSAUBUSTANOO DASSAUBUSTANOO DASSAUBUSTANOO DASSAUBUSTANOO DASSAUBUSTANOO DASSAUBUSTANOO	Factor IP Front End USJ-ovF 2027 ovF 2017 ovF 2019 CGP (mole subst chatter)	Method Bene Bude (50% availability) Bude (50% availability) Bude (50% availability) Bude (50% availability)	8238840258 8238840258 8248840258				
	r.	upyan	9/9/0_53/10P_50	Server Devidencerffort - Action Covidencestremot Devidencestremot Devidencestremot Devidencestremot	Function In FrankEnd SST WF SST WF STP DOT STORE addres (MINO)	Method Donei Dole (50% availabilité Dole (50% availabilité Dole (50% availabilité Dole (50% availabilité Dole (50% availabilité	82883-6255 82883-6288				
	Vacy new Se	faqa									
l c	otherv	6 have been need to rear wise, continue	e with the ne	d with the ograde cycl ext step.	upgrade pl le, see sec	lan show ction 5.2.3	n on the so 3 to do it;	creen.			
u s c t	upgra upgra serve group lf the then r	e are some lir de, which are de options, fe r is not upgra . Identify the DC server dis earrange the upgraded in	e upgraded i or example I ided in first u o DC server i splays by de upgrade cy	n a group o DA-MP, vS upgrade cy using Appe fault in the cles using	of servers. TP MP(s). cle of the (endix N Ide first upgra section 5.2	This is a So, mal C-Level s entify the ade cycle 2.3 such	applicable ke sure the servers in i DC server of its serv that the D0	for all e DC ts server rer group,			
1	vSTP	MPs should	be divided in	n cycles to	avoid a ne	etwork ou	itage.				
N s	MP/v8 serve	cases, regard STP server g r upgraded. ges is minimiz	roup, the DA By upgradin	-MP leade g the MP le	er/vSTP Mi eader last,	Pleader	should be	the last			
		A-MP leader A-MP leader						Yes.			
	Also, CLI.	check for the	MP leader of	on the vST	P. This is	done on	the active	SOAM			
2	4. F	rom the MMI	command u	sing the R	EST Client	t for the v	STP config	guration.			
		he MMI user	guide can a	ccessed by	/ navigatin	g to Maiı	n Menu >∣	ммі			
	9	uiuc.									
				-			Guide.				

Step #	Procedure	Description					
		 The result is the hostname of the MP leader server. 6. In the Upgrade Settings section of the form, use the Upgrade ISO options to select the target ISO. Click OK to start the upgrade sequence. Control returns to the Upgrade 					
3.	Active NOAM VIP: View the upgrade administratio n form to monitor upgrade progress						
		More detailed status is available by selecting the individual server group links. The server group view shows the status of each individual server within the selected server group. During the upgrade, the servers may have a combination of the following expected alarms. Note: Not all servers have all alarms: Alarm ID = 10008 (Provisioning Manually Disabled) Alarm ID = 10073 (Server Group Max Allowed HA Role Warning) Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped) Alarm ID = 31101 (DB Replication To Slave Failure) Alarm ID = 31106 (DB Merge To Parent Failure) Alarm ID = 31107 (DB Merge From Child Failure) Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server) Alarm ID = 31233 (HA Secondary Path Down) Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)					

Step #	Procedure	Description
		Alarm ID = 32515 (Server HA Failover Inhibited) Alarm ID = 31114 (DB Replication over SOAP has failed) Alarm ID = 31225 (HA Service Start Failure) Alarm ID = 31149 (DB Late Write Nonactive)
		<i>Note</i> : Do not accept any upgrades at this time.
		<i>Note</i> : In the unlikely event that after the upgrade, if the Upgrade State of server is Backout Ready and the Status Message displays Server could not restart the application to complete the upgrade , then perform Appendix M Manual Completion of Server Upgrade to restore the server to full operational status and return to this step to continue the upgrade.
		Perform Appendix U to create a link of Comagent.
		If the upgrade fails, do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix I for failed server recovery procedures.
4.	Server CLI: If the	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
	upgrade of a server fails:	 /var/TKLC/log/upgrade/upgrade.log /var/TKLC/log/upgrade/ugwrap.log /var/TKLC/log/upgrade/earlyChecks.log /var/TKLC/log/platcfg/platcfg.log It is recommended to contact My Oracle Support (MOS) by referring to Appendix Z of this document and provide these files. Refer to Appendix I for failed server recovery procedures. When upgrade failure issue is identified and resolved, then Auto Site upgrade can be started again without executing any failed server recovery procedure.
5. □	Post upgrade verification	Proceed to section 5.4 Site Post-Upgrade Procedures for post upgrade verification procedures.

5.2.3 Rearrange Automated Site Upgrade Cycles

This procedure provides details to rearrange the Automated Site Upgrade cycles if required.

Automated Site Upgrade provides an option to rearrange servers in the cycles thus eliminating the risks of a potential network outage. ASU provides the flexibility to user to order the servers within the cycles without breaking the Minimum Availability and DA-MP Leader/vSTP MP leader criteria.

Procedure 20. Rearrangement of upgrade cycles for Automated Site Upgrade

ep#	Procedure	Desci	ription					
	ocedure provides off $()$ each step		-					ach ste
his pr	rocedure fails, it Active		Rearrange Cy		le Support (N	1OS) and as	k for assis	tance.
	NOAM VIP:	CIICK	tean ange og	y cies.				
F ti	Rearrange	Main Me	enu: Administration	-> Software Managem	ent -> Upgrade [Sit	e Initiate]		
	the upgrade	ielo" >	1					
	cycle as	Cycle	Action	Servers				
	needed	•	Cpgrade	Server Group Stevel_BOAM_SG	Sacver DerSite(OSOAMOII - Standta	Function DBR (active/standity pair)	Nethod Version OAM (Bullo B.2.0.5.0-8	258
		2	Upgrade	Sorver Group Tankot_PFIE_E0_0 SHK01_BSTMP_B0 SHK03_STMP_B0 SHK03_DWP_S0	0 Dw5re01657MP00	Fraction IF front End SS3 will SS3 will SS	Hethod Serial Bula (30% availability) Bula (30% availability) Bula (30% availability) Bula (30% availability)	82000-025
		3	t by ada		2 Diversion (SSTMPO) 3 Diversion (SSTMPO)	Function IF Front End SST-ANF SST-ANF STP DBR imulti-active studies	Method Gertal Bute (52% availability Bute (52% availability Bute (52% availability Bute (52% availability)	820004251 820004251
			iethigs 00 069-0.2000,827,0-0 Cancel Reamange Cycles IN	6,66.100 🛨 Selective desired up	ignade ISO media lite			
2.	Active NOAM VIP: Rearrangem ent of Servers in cycles	1. Au Note :	Only DA-MI	Upgrade Cycle Ps, and vSTPs, rs is restricted.			-arranging) SBR a

itep #	Procedure		ription Menu: Administrati	ion -> \$	Software Manag	agement -> Upgrade [Rearrange Cycles]
		Cycle	Available Server			Free Pool
			Server	1	Action	2
		1	DerSite00504M00	- 2	Adult To Cyclin	
				E	Remove From Cycle	
			Server	T I	Action	
	Z	z	DerSite00557MP00 DerSite00557MP01 DerSite00557MP01 DerSite0057PMP01 DerSite0057PMP01	The second secon		
		Server	P	Action		
		3	DerSite00(PPED) DerSite00SS7MP02 DerSite00SS7MP03 DerSite00STPMP00 DerSite00STPMP00	4	Antil To Cycle Harmovie Friten Cycle	
		OK	Cancel Add Cycle		Ê.	2
			/hen a server nee			from cycle and needs to be added i his:
		1				st and click Remove from Cycle .
			The server Mo	ves to	the Free Poo	ol on the right side.

Step #	Procedure	Desc	ription					
		Main	Menu: Administratio	n ->	Software Manag	gement -> Upgrade [Rearrange Cycles]	
		Cycle	Available Server			Free Pool		
						DarSite00657MP02 DarSite00557MP01	2	
		1	DerSm0050AM00	4	Action Add To Cycle			
				×	Plemove Fram Cycle			
		_	Senar	Server Action OprStee00575/MP00 DerStee00577MP01 DerStee0057FMP01 OprStee000AMP02 OveCtm200AM900				
		2	DerSite000FFE00 DerSite00557MP00 DerSite0057PMP01 DerSite00DAMP02					
			Server		Action			
		3	DerSite00FFE01 DerSite00SS7MP03 DerSite00STFMP00 DerSite00DAMP03	-	Add To Cycle			
				2			-1	
		OR.	Cancel Add Cycle					
		2				another existing	cycle or new cycle. , if required	
			there is no need	to a	idd a new cyd	cle, then steps to	rearrange the cycle are ted to this procedure.	

Step #	Procedure	Des	Description							
3. □	Active NOAM VIP: Add new		1. Click Add Cycle. Main Menu: Administration -> Software Management -> Upgrade [Rearrange Cycles]							
	cycle (If required)		2	Remove From Cycle	21					
			Server	Action						
		z	DerSte00PTE00 DerSte00957MP00 DerSte005TPMP01	Auto To Cyclin						
			DarShe000AMP02	Buonove From Cyclu						
			Server	Action						
		3	DerSte0027501	Auto To Cyclin						
			DerStee000AMP03	Terminen Frank Cycler						
			Server	Action						
		4	DerSite00957MP02	auto To Cycle						
			2	Romove From Cycle						
			Server	Action						
			DerSite005574P01	Aill to Cycle						
			-	Hernove From Cyclic						
			Server	Action	*					
			-	Aului To Cytole						
			Q z	Furnishin Frank Cycle						
		OR	Cancel Anti Cycle							
			After adding new c cycle. Click OK .	ycle, servers a	available in free pool can be added in new					

5.3 Automated Server Group/Manual Upgrade Overview

This section contains alternative site upgrade procedures that can be used when Automated Site Upgrade does not meet the needs or concerns of the customer. These procedures use a combination of Automated Server Group upgrade and manual server upgrades to upgrade a specific site.

Table 13 details the site upgrade plan for a non-PCA/PDRA site, which divides the upgrade into four cycles. A cycle is defined as the complete upgrade of one or more servers, from initiate upgrade to success or failure. The first two cycles consist of upgrading the SOAMs - the first cycle upgrades the standby SOAM, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures that the OAM controllers are always upgraded before any C-level servers.

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, vSTP MPs, and IPFEs are upgraded. This leaves the remaining half of these server functions in-service to process traffic. The fourth cycle upgrades the second half of the DA-MPs, and IPFEs to complete the site upgrade.

Cycle 1	Cycle 2	Cycle 3	Cycle 4
Standby SOAM	Active SOAM		
		½ DA-MPs	1⁄2 DA-MPs
		½ IPFEs	1/2 IPFEs
		½ vSTP MPs	1/2 vSTP MPs

Table 13. Non-PCA/PDRA Site Upgrade Plan	۱
--	---

Table 14 details the site upgrade plan for a PCA/PDRA system with two-site redundancy. This upgrade plan is divided into five cycles. The first two cycles consist of upgrading the SOAMs - the first cycle upgrades the standby and spare SOAMs in parallel, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures that the OAM controllers are always upgraded before any C-level servers.

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, IPFEs, and vSTP servers are upgraded in parallel with all of the spare SBRs. This leaves the remaining server functions in-service to process traffic.

The fourth cycle upgrades the second half of the DA-MPs, and IPFEs in parallel with the standby SBRs.

The fifth cycle is required to upgrade the active SBR(s), completing the site upgrade.

Cycle 1	Cycle 2	Cycle 3	Cycle 4	Cycle 5
Standby SOAM, Spare SOAM	Active SOAM			
		½ DA-MPs	½ DA-MPs	
		1/2 IPFEs	½ IPFEs	
		Spare SBR(s)	Standby SBR(s)	Active SBR(s)

 Table 14. Two-Site Redundancy PCA Site Upgrade Plan

Table 15 details the site upgrade plan for a PCA/PDRA system with three-site redundancy. This upgrade plan is divided into six cycles.

Note: It is mandatory to follow the mentioned division and execution order of the cycles. This ensures the OAM controllers are always upgraded before any C-level servers.

For C-level servers, the division of servers can be planned in different cycles depending on customer requirements, which means SBR and DA-MPs can be upgraded in different cycles. **But, as mentioned, spare, standby, and active SBRs should be upgraded in different cycles.**

The first two cycles consist of upgrading the SOAMs – the first cycle upgrades the standby and spare SOAMs in parallel, followed by the second cycle, which upgrades the active SOAM. Cycle 3 cannot begin until cycle 2 is complete. This ensures the OAM controllers are always upgraded before any C-level servers.

The third cycle begins the upgrade of the C-level servers. In cycle 3, one-half of the DA-MPs, and IPFEs are upgraded in parallel with one spare SBR. This leaves the remaining server functions in-service to process traffic.

The fourth cycle upgrades the second half of the DA-MPs, and IPFEs in parallel with the second spare SBR.

The fifth cycle upgrades the standby SBR(s), and the sixth cycle is required to upgrade the active SBR(s), completing the site upgrade.

Table 15. Three-Site Redundancy PCA Site Upgrade Plan

Cycle 1	Cycle 2	Cycle 3	Cycle 4	Cycle 5	Cycle 6
Standby SOAM, Spare SOAM	Active SOAM				
		1/2 DA-MPs 1/2 DA-MPs			
		1/2 IPFEs	1/2 IPFEs		
		Spare SBR(s)	Spare SBR(s)	Standby SBR(s)	Active SBR(s)

5.3.1 Site Upgrade Planning

The upgrade of the site servers consists of a mixture of automated upgrades using the Automated Server Group upgrade feature, along with "manual" upgrades that are a little less automated.

Table 16 should be used to plan the upgrade of each site. For the server groups that are upgraded using ASG, the only planning necessary is to record the server group name. ASG automatically selects the individual servers to upgrade. The IPFE, and vSTP (if equipped) server groups must be upgraded manually since there is only one server per server group. Planning is necessary for these server groups to ensure traffic continuity. Record the hostname of the servers to be upgraded in each iteration. vSTP MPs should be divided in cycles to avoid a network outage.

While choosing ASG and Manual upgrades for multi-active MP servers, see the limitations in Appendix O for the Automated Server Group upgrade option.

If your network aligns with any of the scenarios listed in Appendix O, then do NOT use the Automated Server Group. This avoids risks of a potential network outage.

There are some limitations with upgrading the DC server in a C-level server group, which are upgraded in a group of servers, for example, DA-MP, vSTP MP(s). So, make sure the DC server is not upgraded in first upgrade cycle of the C-Level servers in its server group. Identify the DC server using Appendix N Identify the DC server.

In all cases, regardless of the number of cycles used to upgrade the DA-MP/vSTP server group, the DA-MP leader/vSTP MP leader should be the last server upgraded. By upgrading the MP leader last, the number of leader changes is minimized during the upgrade.

The DA-MP leader is designated on the active SOAM at **Diameter > Maintenance > DA-MPs > Peer DA-MP Status**, where **MP Leader = Yes**.

Also, check for the MP leader on the vSTP. This is done on the active SOAM CLI.

1. From the MMI command using the REST Client for the vSTP configuration.

The MMI user guide can accessed by navigating to Main Menu > MMI Guide.

2. Use the /vstp/mpleader MO.

The result is the hostname of the MP leader server.

Table 16. Site Upgrade Planning Sheet

Iteration 1		Notes
Standby SOAM Hostname Spare SOAM Hostname		If a spare SOAM exists, the spare and standby SOAMs are upgraded manually. Otherwise, the SOAMs are upgraded with ASG.

Iteration 1	Notes
Iteration 2	Notes
Active SOAM	The active SOAM is upgraded in iteration 2, either manually or by ASG.
Iteration 3	Notes
DA-MP Group 1	ASG automatically selects DA-MPs for upgrade
IPFE 1 Hostname	Manual upgrade
IPFE 3 Hostname	Manual upgrade
Spare SBR(s)	ASG automatically selects the spare SBR(s) for upgrade
Iteration 4	Notes
DA-MP Group 2	ASG automatically selects DA-MPs for upgrade
IPFE 2 Hostname	Manual upgrade
IPFE 4 Hostname	Manual upgrade
Standby SBR(s)	ASG automatically selects the standby SBR(s) for upgrade
Iteration 5	Notes
Active SBR(s)	ASG automatically selects the active SBR(s) for upgrade

Table 17 shows the procedures to be executed for the site upgrade, along with the estimated time to complete each step. Use Table 17 as a guide for determining the order in which the procedures are to be executed.

	Elapsed Time (hr:min)			
Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 14	0:10-0:20	0:10-0:20	Procedure 14	None
Procedure 16	0:05-0:10	0:15-0:30	Site Upgrade Options Check	None
Procedure 16	0:01-0:05	0:16-0:35	Site Upgrade Options Check	Site Provisioning Disabled, No Traffic Impact
Procedure 21	0:01-0:05	0:17-0:40	SOAM Upgrade Pre-Checks	No Traffic Impact
Iteration 1	0:40-1:00	0:57-1:40	Standby SOAM, Spare SOAM (if equipped)	Refer to Section 5.3.2 for details
Iteration 2	0:40-1:00	1:37-2:40	Active SOAM	Refer to Section 5.3.2 for details
Iteration 3	0:40-1:00	2:17-3:40	1/2 DA-MPs, 1/2 IPFEs, Spare SBR(s), 1/2 vSTP MPs	Refer to Section 5.3.4 for details
Iteration 4	0:40-1:00	2:57-4:40	1/2 DA-MPs, 1/2 IPFEs, Standby SBR(s), 1/2 vSTP MPs	Refer to Section 5.3.5 for details
Iteration 5	0:00-1:00	2:57-5:40	Active SBR(s)	Refer to Section 5.3.6 for details
Procedure 27	0:02	2:59-5:42	Allow Site Provisioning	Site Provisioning Enabled, No Traffic Impact
Procedure 28	0:10-0:15	3:09-5:57	Site Post-Upgrade Health Check	None

Table 17.	Site U	parade	Execution	Overview
	0.000	pgiaao	EXCOUNTION	010111011

5.3.2 SOAM Upgrade Overview

This section contains the steps required to perform a major or incremental upgrade of the SOAMs for a DSR site.

During the site upgrade (SOAMs plus all C-level servers), site provisioning is disabled. Provisioning is reenabled at the completion of the site upgrade.

For each site in the DSR, the SOAM(s) and associated MPs and IPFEs should be upgraded within a single maintenance window.

Table 18 shows the estimated execution times for the SOAM upgrade. Procedure 23 is the recommended procedure for upgrading the SOAMs when there is no spare SOAM. ASG automatically upgrades the standby SOAM followed by the active SOAM.

If the site does have a spare SOAM, Procedure 23 is the recommended procedure. The manual upgrade procedure upgrades the standby and spare SOAMs in parallel, followed by the active SOAM.

Note: For information on SOAM VM profile for increased MP Capacity, refer to Appendix V.

Table 18. SOAM Upgrade Execution Overview

Procedure	Elapsed Tir	ne (hr:min)	Procedure Title	Impost
Procedure	This Step	Cum.		Impact
Iteration 1 & 2	1:20-2:40	1:20-2:40		No traffic
Procedure 22			Procedure 22	impact
or				
Procedure 23			Procedure 23	

5.3.3 Upgrade SOAMs



This section provides the procedures to upgrade the SOAMs. The SOAMs can be upgraded manually under user control, or automatically using the Automated Server Group Upgrade option. The recommended method for SOAM upgrade depends on the existence of a spare SOAM. If the site includes a spare SOAM, then the SOAMs are upgraded manually so that the spare and standby can be upgraded concurrently. This reduces the time required to upgrade the SOAMs.

Regardless of which SOAM upgrade option is used, Procedure 21 SOAM Upgrade Pre-Checks is required to ensure site provisioning is disabled.

If the site does not include a spare SOAM, use the automated SOAM upgrade in Procedure 22.

If the site does include a spare SOAM, use the manual SOAM upgrade in Procedure 23.

Procedure 21. SOAM Upgrade Pre-Checks

Step #	Procedure	Description			
upgradir Check c number	This procedure verifies traffic status, and verifies that Site Provisioning is disabled, in preparation for upgrading the SOAMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	Active SOAM VIP: View KPIs to verify traffic status	 Log into the active SOAM GUI using the VIP. Navigate to Status & Manage > KPIs. Inspect KPI reports to verify traffic is at the expected condition. 			
2.	Active SOAM VIP: Verify Site Provisioning is disabled	Verify that Site Provisioning was properly disabled in Procedure 17. In the GUI status bar, where it says Connected using , check for the message Site Provisioning disabled . If the message is present, continue with the next procedure per Table 17; otherwise, execute Procedure 17.			

5.3.3.1 Automated SOAM Upgrade (Active/Standby)

Procedure 22 is the recommended method for upgrading the SOAMs if the site does not include a spare SOAM. If the site has a spare SOAM, upgrade using Procedure 23. Upon completion of this procedure, proceed to Section 5.3.4 Upgrade Iteration 3.

Step #	Procedure	Description			
Check of number.	 This procedure upgrades the SOAM(s) using the Automated Server Group Upgrade option. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance. 				
1.	Upgrade SOAM Server Group	 Upgrade the SOAM server group using the Upgrade Multiple Servers procedure with the following options: Use the Automated Server Group Upgrade option Select the Serial upgrade mode Execute Appendix D Upgrade Multiple Servers – Upgrade Administration. After successfully completing the procedure in Appendix D, return to this point and proceed to section 5.3.4 Upgrade Iteration 3. 			

Note: Once the network element SOAMs are upgraded, if any C-level server is removed from a server group and re-added, the server must be restored using disaster recovery procedures. The normal replication channel to the C-level server is inhibited due to the difference in release versions.

5.3.3.2 Manual SOAM Upgrade (Active/Standby/Spare)

Procedure 23 upgrades the SOAM server group if the site includes a spare SOAM. If the SOAM server group was upgraded using Procedure 22, then do not execute this procedure; proceed to section 5.3.4 Upgrade Iteration 3.

Procedure 23. Manual SOAM Upgrade (Active/Standby/Spare)

Step #	Procedure	Description		
 This procedure upgrades the SOAMs in a DSR manually. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance. 				
1.	Upgrade standby and spare SOAMs in parallel using the Upgrade Multiple Servers procedure	Execute Appendix D Upgrade Multiple Servers – Upgrade Administration. After successfully completing the procedure in Appendix D, return to this point and continue with the next step.		
2.	Upgrade active SOAM using Upgrade Single Server procedure	Execute Appendix C Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and proceed to section 5.3.4 Upgrade Iteration 3.		

Note: Once the network element SOAMs are upgraded, if any C-level server is removed from a server group and re-added, the server must be restored using disaster recovery procedures. The normal replication channel to the C-level server is inhibited due to the difference in release versions.

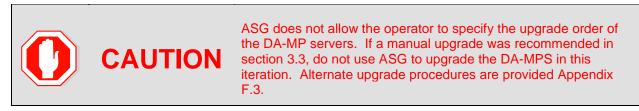
5.3.4 Upgrade Iteration 3

Upgrade iteration 3 begins the upgrade of the site C-level servers. As shown in Table 16, iteration 3 consists of upgrading the DA-MPs, IPFEs, spare SBR(s), and vSTP MP server, if equipped. The C-level components are upgraded in parallel to maximize Maintenance Window usage.

Table 19 shows the estimated time required to upgrade the C-level servers for iteration 3.

	Elapsed Time (hr:min)			
Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 24	0:40-1:00	0:40-1:00	Procedure 24	1/2 DA-MPs, 1/2 IPFEs, spare SBR(s), 1/2 vSTPs servers will be offline

 Table 19. Iteration 3 Upgrade Execution Overview



Procedure 24 upgrades $\frac{1}{2}$ of the DA-MPs, $\frac{1}{2}$ of the IPFEs, $\frac{1}{2}$ of the vSTPs, and the spare SBR(s). Refer to Table 16 for the hostnames of the servers to be upgraded in this iteration.

Procedure 24. Upgrade Iteration 3

	. •					
Step #	Procedure	Description				
This pro	cedure upgrades a	a portion of the C-level servers for iteration 3.				
Check o number.	• • •	it is completed. Boxes have been provided for this purpose under each step				
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	Active NOAM	1. Log into the NOAM GUI using the VIP.				
	VIP: Select the DA-MP	2. Navigate to Administration > Software Management > Upgrade.				
	server group to	3. Select the SOAM tab of the site being upgraded.				
	view pre- upgrade status 4. Select the DA-MP Server Group link.					
	of DA-MPs	5. For the DA-MP servers to be upgraded in iteration 3, verify the application version value is the expected source software release version.				

Step #	Procedure	Description					
□ VIP : View pi	0. 27	Backup. T the backup 2. Verify the O	ne Upgrade s is complete, AM Max HA This depends	State change the Upgrade Role is in th on the serv	es to Backup State chang he expected er being upg	o in Prog ges to Ro conditior raded. rade	vers and click gress. When eady. n (either standby
		Hostname	Upgrade State Server Status	OAM HA Role	Server Role Network Element	Function	Application Version
		N02	Ready	Active N/A	Network OAM&P	OAM&P	8.0.0.0.0-80.25.0
		NOT	Failed Norm	Standby N/A	Network OAM&P NE_NO	OAM&P	800.0.0-80.250 DSR-8.3000_83.3.7-
		e Backup Backup All	Checkup Checku	o All Auto Upgred	e Accept Repo	rt Report A	,

Step #	Procedure	Description						
3.	Active NOAM VIP: Verify upgrade status is Ready for	This may take a being upgraded, The Upgrade Ad group of the site	new alarms ministration	may occur. screen disp		, ,		
	the server to be upgraded	Main Menu: Admin	nistration -> S	oftware Mana	gement -> Upg	rade	2	
		Filter* + Tasks +						
		NO_SO SO_East	SO_North SO_We	st, (
		Entre Site SO_East	IPFE1_BG IPFE	2_8G IPFE3_8G	IPFE4_SG MP_S	1		
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO	
		мРЗ	Ready	Active	MP	DSR (multi- active cluster)	7.2.0.0.0-72.25.0	
			Norm	Active	SO1_DSR_VM			
		MP4	Ready	Standby	MP	DSR (multi- active cluster)	7 2 0 0 0-72 25 0	
			Norm	Active	SO1_DSR_VM			
		MP1	Ready	Standby	MP	DSR (multi- active cluster)	7,2.0.0.0-72.25.0	
			Norm	Active	SO1_DBR_VM	-		
		MP2	Ready	Standby	MP	DSR (multi- active cluster)	7.2.0.0.0-72.25.0	
			Norm	Active	SO1_DSR_VM			
		Alarm II Alarm II Alarm II	ervers have D = 10008 (F D = 10073 (\$ D = 10075 (1	all alarms: Provisionin Server Grou Fhe server i	g Manually I up Max Allov is no longer	Disabled ved HA ∣ providiı	l) Role Warning	
		Alarm I) = 32515 (S	Server HA F	ailover Inhi	bited)		
		Alarm ID = 31101 (DB Replication to slave DB has failed)						
		Alarm ID = 31106 (DB Merge to Parent Failure)						
			•	•	rom Child F			
					vailable ser		d to receive ate Server)	
		Alarm I) = 31114 (I	DB Replicat	ion over SO	AP has	failed)	
		Alarm I) = 31225 (ł	A Service	Start Failure	2)		

Step #	Procedure	Description					
4 .	Active NOAM VIP: Initiate the Automated Server Group upgrade of the DA-MP servers (part 1)		group are sel Upgrade .	ected.		rade	ify no servers in
		Hostname NO2 NO1	Upgrade State Server Status Ready Err Failed Norm	OAM HA Role Appl HA Role Active NVA Standby NVA	Server Role Network Element Network OAM&P NE_NO Network OAM&P NE_NO	CAMSP CAMSP	Application Version Upgrade ISO 8.0.0.0-80.25.0 8.0.0.0-80.25.0 DSR-8.3.0.0.0_83.3.7-4
5.	Active NOAM VIP: Initiate the Automated Server Group upgrade of the DA-MP server (part 2)	of the serve 2. Select 50% 3. Select the a 4. Click OK to Upgrade Settings Wode Black Bulk Soma G Grouped B Available 50%	er group upg o for the Avai appropriate Is o start the upg	section of the rade. Select lability setti SO from the grade. Server group upgrad Select "Bulk" to upgr Select	ne Initiate scre t Bulk Mode. ing. Upgrade ISC Upgrade ISC upgrade servers in KA signated servers in KA signated servers in KA signated tast server will be ad according to the "Applica spars, observed, standby ar	C option	rols the behavior S. ability setting in HA order g to the availability setting. the server

Step #	Procedure	Description								
6.	Active NOAM VIP: View the	Observe the upgrade state of the DA-MP servers. Upgrade status displays under the Status Message column.								
	upgrade	Main Menu: Administration -> Software Management -> Upgrade								
	administration form to monitor	Filter* • Status • Tasks •								
	upgrade	NO_SB SO_Enet SO_North SO_Weat								
	progress	Entre Ste SO_East IPFE1_SO IPFE1_SO IPFE4_SO MP 5G								
		Hostname Upgrade State DAM HA Role Server Role Function Application Version Server Status Appl HA Role Network Element Upgrade ISO								
		NP1 Upgrading Standby MP OSR (multi- active 7 2 0.0 0-72 35 0								
		NET Clustery Clustery DSR-8.0.0.0.90.10.0-vi86_64.iso								
		NP2 Pending Active NP DSR (mult- active 7.2.0.0.0-72.25.0 cluster)								
		Ex Active SO1_DSR_VM DSR-8.0.0.0.0_80.18.0+x86_64.ee								
7.	Identify the	upgrade additional C-level components in parallel. From the data captured in Table 16, identify the IPFE server group(s) to								
	IPFE server group(s) to upgrade	upgrade in iteration 3.								
8.	group(s) to	 upgrade in iteration 3. 1. Navigate to Administration > Software Management > Upgrade. 								
8.	group(s) to upgrade Active NOAM VIP: View pre-	 Navigate to Administration > Software Management > Upgrade. 								
8.	group(s) to upgrade Active NOAM	 Navigate to Administration > Software Management > Upgrade. 								
8.	group(s) to upgrade Active NOAM VIP: View pre- upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. 								
8.	group(s) to upgrade Active NOAM VIP: View pre- upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Select the link for each IPFE server group to upgrade. For the IPFE servers to be upgraded in iteration 3, verify the application 								
8.	group(s) to upgrade Active NOAM VIP: View pre- upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Select the link for each IPFE server group to upgrade. For the IPFE servers to be upgraded in iteration 3, verify the application version value is the expected source software release version. If a server is in Backup Needed state, select the servers and click Backup. The Upgrade State changes to Backup in Progress. When the backup is complete, the Upgrade State changes to Ready. Verify the OAM Max HA Role is in the expected condition (either standby) 								
8.	group(s) to upgrade Active NOAM VIP: View pre- upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Select the link for each IPFE server group to upgrade. For the IPFE servers to be upgraded in iteration 3, verify the application version value is the expected source software release version. If a server is in Backup Needed state, select the servers and click Backup. The Upgrade State changes to Backup in Progress. When the backup is complete, the Upgrade State changes to Ready. Verify the OAM Max HA Role is in the expected condition (either standby or active). This depends on the server being upgraded. 								
8.	group(s) to upgrade Active NOAM VIP: View pre- upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Select the link for each IPFE server group to upgrade. For the IPFE servers to be upgraded in iteration 3, verify the application version value is the expected source software release version. If a server is in Backup Needed state, select the servers and click Backup. The Upgrade State changes to Backup in Progress. When the backup is complete, the Upgrade State changes to Ready. Verify the OAM Max HA Role is in the expected condition (either standby or active). This depends on the server being upgraded. 								
8.	group(s) to upgrade Active NOAM VIP: View pre- upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Select the link for each IPFE server group to upgrade. For the IPFE servers to be upgraded in iteration 3, verify the application version value is the expected source software release version. If a server is in Backup Needed state, select the servers and click Backup. The Upgrade State changes to Backup in Progress. When the backup is complete, the Upgrade State changes to Ready. Verify the OAM Max HA Role is in the expected condition (either standby or active). This depends on the server being upgraded. 								
8.	group(s) to upgrade Active NOAM VIP: View pre- upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Select the link for each IPFE server group to upgrade. For the IPFE servers to be upgraded in iteration 3, verify the application version value is the expected source software release version. If a server is in Backup Needed state, select the servers and click Backup. The Upgrade State changes to Backup in Progress. When the backup is complete, the Upgrade State changes to Ready. Verify the OAM Max HA Role is in the expected condition (either standby or active). This depends on the server being upgraded. 								
8.	group(s) to upgrade Active NOAM VIP: View pre- upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Select the link for each IPFE server group to upgrade. For the IPFE servers to be upgraded in iteration 3, verify the application version value is the expected source software release version. If a server is in Backup Needed state, select the servers and click Backup. The Upgrade State changes to Backup in Progress. When the backup is complete, the Upgrade State changes to Ready. Verify the OAM Max HA Role is in the expected condition (either standby or active). This depends on the server being upgraded. 								
8.	group(s) to upgrade Active NOAM VIP: View pre- upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Select the link for each IPFE server group to upgrade. For the IPFE servers to be upgraded in iteration 3, verify the application version value is the expected source software release version. If a server is in Backup Needed state, select the servers and click Backup. The Upgrade State changes to Backup in Progress. When the backup is complete, the Upgrade State changes to Ready. Verify the OAM Max HA Role is in the expected condition (either standby or active). This depends on the server being upgraded. 								

Step #	Procedure	Description					
9.	Active NOAM VIP: Verify upgrade status is Ready for	This may take being upgrade The Upgrade group being up	d, new alarms Administratior	s may occui	r.	·	g on the server e IPFE server
	the server to	<u> </u>	ninistration -> S	offware Mana	cement -> Unc	rade	
	be upgraded			Univere maria	gement -> opg	aue	
		Filter* + Tasks	•				
		NO_SG SO_East	SO_North SO_Wes				Laborator Obstantion
		Entire Site SO_Ear	2 [1007 927] Date	.962 IPFE_863	IPFE_SG4 MP_SC		\$\$7_\$61 \$\$7_\$62
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
		IPFE1	Ready	Active	MP	IP Front End	7.3.0.0.0-73.18.0
		IFFEI	Norm	N/A	SO1_DSR_VM		
		Servers may h	ave a combin	ation of the	following ex	pected a	larms.
			l servers have		•		
		Alarm	ID = 10008 (Provisionir	ng Manually	Disable	d)
		Alarm	ID = 10073 (Server Gro	oup Max Allo	wed HA	Role Warning)
		Alarm	ID = 10075 (The server	is no longe	r provid	ing services
		becau	ise applicatio	on process	es have bee	n manua	ally stopped)
		Alarm	ID = 32515 (Server HA	Failover Inh	ibited)	
			ID = 31101 (-			s failed)
		Alarm	ID = 31106 (DB Merge	to Parent Fa	ilure)	
		Alarm	ID = 31107 (DB Merge I	From Child I	Failure)	
							ed to receive
			heartbeats) c	•			-
			ID = 31114 (-			s ralled)
		Alarm	ID = 31225 (HA Service	e Start Fallur	e)	
10.	Active NOAM	Select the Upg	grade Server i	method.			
	VIP: Initiate IPFE upgrade	1. From the l	Jpgrade Adm	inistration s	creen, select	the serv	er to upgrade.
	(part 1)	2. Click Upg	rade Server.				
		Main Menu: Adr	ministration -> S	oftware Mana	igement -> Upg	rade	6
		Filter* • Tasks	•				
		and the second					
		NO_SG SO_East	SO_North SO_We				and the second second
		Entre Site SO_Ea		_SG2 IPFE_SG3	IPFE_SG4 MP_S0		\$87_\$G1 \$\$7_\$G2
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
	OVERECC)	Ready	Active	MP	IP Front End	7.2.0.0.0-72.25.0	
		IPFE1	Norm	NIA	S01_DSR_VM	1	

Step #	Procedure	Description						
11.	Active NOAM VIP: Initiate IPFE upgrade (part 2)	 Select target ISO. 1. On the Upgrade Initiate screen, select the target ISO from the Upgrade ISO options. 2. Click OK to start the upgrade. Main Menu: Administration -> Software Management -> Upgrade [Initiate] Info* • Hostname Action Status OAM HA Role Appl HA Role Network Element						
		IPFE1 Upgrade Active N/A SO1_DSR_VM						
		Upgrade Settings						
		Upgrade ISO DSR-8.0.0.0_80.20.0-x86_64.iso Select the desired upgrade ISO media file.						
12.	Active NOAM VIP: View the upgrade administration form to monitor upgrade progress	Observe the upgrade state of the IPFE server. Upgrade status displays under the Status Message column. Main Menu: Administration -> Software Management -> Upgrade Filter* Status * Tasks * NO_90 SO_East SO_North SO_West Entre Ste SO_East SO_North SO_West Hostsame Upgrade State OAM HA Role Server Role Function Application Version Server Status Appl HA Role Network Element Upgrade ISO MP IP Front End 7.3.0.0.0_B0.20.0-x36_54.lso						
13. □	Repeat for each IPFE	Repeat steps 7. through 12. for the next IPFE to be upgraded in this iteration per Table 16.						
14.	Identify the SBR server group(s) to upgrade	From the data captured in Table 16, identify the SBR server group(s) to upgrade in iteration 3. ASG steps (Auto Upgrade), mentioned in the next steps, do not provide any liberty to the operator to verify observations during the upgrade. If a manual upgrade was recommended for the SBR upgrade, do not use ASG to upgrade all the SBR servers from the same server group in this single iteration. Alternate upgrade procedures are provided in Procedure 52. Spare SBR server(s) need to be upgraded. If the Manual Upgrade is used, skip ASG steps 15. to 19.						

Step #	Procedure	Description								
15.	Active NOAM	1. Navigate to Administra	tion > Software Manage	ement >	Upgrade.					
	☐ VIP: View pre- upgrade status of SBRs to upgrade	2 Select the SUAW tab of the site being upgraded								
		of SBRs to 3. Select the link for each SBR server group to upgrade.								
		4. For the SBR servers to a version value is the expe								
		 If the server is in Backu Backup. The Upgrade the backup is complete, Verify the OAM Max HA or active). This depends 	State changes to Backu the Upgrade State chan Role is in the expected	p in Prog ges to Re conditior	gress. When eady.					
		Main Menu: Administration -> S Filter Tasks - NO_80 SO Eest 80_North SO_We	oftware Management -> Upg							
		Entire Sile SO_East IPFE_SG1 IPFE	SG2 IPFE_SG3 IPFE_SG4 MP_S	G SBR.5G	\$\$7_\$G1 \$\$7_\$G2					
		Hostname Upgrade State Server Status	OAM HA Role Server Role Appl HA Role Network Element	Function	Application Version					
		SBR2 Backup Needed	and the second s	SBR	7.3.0.0.0-73.18.0					
		Backup Needed	Spare SO1_DSR_VM	SBR	7.3.0 0.0-73 18 0					
		SBR3 Norm	Active SO1_DSR_VM							
		SBR1	Spare MP	SBR	7.3.0.0.0-73 18.0					
				CONTRACTOR CONTRACTOR IN						

Step #	Procedure	Description							
16. □	Active NOAM VIP: Verify upgrade status is Ready for the server to	This may take a being upgraded, The Upgrade Ac group being upg	new alarms	may occur.					
	be upgraded	Main Menu: Admi	nistration -> S	oftware Mana	gement -> Upgr	ade		-	
		Filter* • Tasks •							
		NO_SG SO_East	SO_North SO_Wes	it .					
		Entire Site SO_East	IPFE_SG1 IPFE	962 IPFE_963	IPFE_SG4 MP_SG	SBR_SG	S\$7_\$G1	\$\$7_\$62	
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Upgrade 15/		
		SBR2	Ready	Active	MP	SBR	7.3.0.0.0-73	18.0	
		3562	Norm	Spare	SO1_DSR_VM				
		SBR3	Ready	Standby	MP	SBR	7.3.0.0.0-73	18.0	
			Norm	Active	SO1_DSR_VM		1		
		SBR1	Ready	Spare Spare	MP SO1_DSR_VM	SBR	7:3.0.0.0-73	18.0	
		Alarm I	ervers have D = 10008 (F	all alarms: Provisionin	g Manually D	isabled	I)	orning)	
		Alarm II becaus	D = 10075 (1 e applicatio	The server i n processe	up Max Allow is no longer es have been	orovidiı manua	ng serv	ices	
		Alarm I	D = 32515 (S	Server HA F	ailover Inhib	ited)			
		Alarm ID = 31101 (DB Replication to slave DB has failed) Alarm ID = 31106 (DB Merge to Parent Failure)							
		Alarm ID = 31107 (DB Merge From Child Failure)							
			•		vailable serv				
		Alarm I	D = 31114 (I	DB Replicat	tion over SO	AP has	failed)		
		Alarm I	D = 31225 (H	A Service	Start Failure		-		

Step #	Procedure	Description							
17.	Active NOAM VIP: Initiate SBR upgrade (part 1)		Upgrade me Automated S ip to upgrade	Server Grou	ıp upgra	de opt	ion, sel	ect the SBR	
	(part I)	-	ervers in the	server grou	ip are se	lected			
		3. Click Auto	Upgrade.						
		Main Menu: Adm	inistration -> S	oftware Man	agement -	> Upgra	ade		
		Filter - Tasks -	.]						
		NO_SG SO_East	SO_North SO_We	st					
		Entre Site SO_East	IPFE_SG1 IPFE	_SG2 IPFE_SG3	IPFE_SG4	MP_SG	SBR SG	\$\$7_\$G1 \$\$7_\$G2	
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Ro Network E		Function	Application Version Upgrade ISO	
		SBR1	Ready	Standby	MP SD1_DSR		SBR	7.3.0.0.0-73.14,0	
		SBR2	Ready Nom	Active Standby	MP SO1_DSR		SBR	7.3.0.0.0-73.14.0	
		SBR3	Ready	Spare	MP		SBR	7.3.0.0.0-73.14.0	
		<	(NORTH)	Spare	SO1_DSR	_vw			
				-	~				
		Backup Backup All	Checkup Checku	ap All Auto Uppr	ade Accept	Report	Report Al	N	
18.	Active NOAM VIP: Initiate		de Settings s	ection of th	e Initiate	scree		Jpgrade. ols the behavio	
18.		 The Upgrad of the autor Select the a 		ection of th de. Select SO from the	e Initiate Serial m	e scree iode.	en contr	ols the behavio	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a 	de Settings s mated upgrad appropriate I start the upg	ection of th de. Select SO from the grade.	e Initiate Serial m e Upgrae	e scree iode. de ISC	option	ols the behavio	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a Click OK to 	de Settings s mated upgrad appropriate I start the upg	ection of th de. Select SO from the grade.	e Initiate Serial m e Upgrae	e scree iode. de ISC	option	ols the behavio	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a Click OK to Main Menu: Admini 	de Settings s mated upgrad appropriate I start the upg	ection of th de. Select SO from the grade.	e Initiate Serial m e Upgrae	e scree iode. de ISC	option	ols the behavio	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a Click OK to 	de Settings s mated upgrad appropriate I start the upg start the upg	ection of th de. Select SO from the grade. are Manageme	e Initiate Serial m e Upgrae	e scree iode. de ISC	option	ols the behavio	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a Click OK to Main Menu: Adminition Hostname Action 	de Settings s mated upgrad appropriate I start the upg start the upg	ection of th de. Select SO from the grade. are Manageme Status OAM HA Rok	e Initiate Serial m e Upgrae nt -> Upgra	e scree node. de ISC de [initia	en contr) option ate] ////	Tue feb 57 13:10 Application Version	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a Click OK to Main Menu: Admini Info Hostname Action SUR1 Auto upgrad 	de Settings s mated upgrad appropriate I start the upg start the upg	ection of th de. Select SO from the grade. are Manageme Status OAM HA Role tareby	e Initiate Serial m e Upgrad nt -> Upgrad Appl HA Role	e scree node. de ISC de [Initia Network E so1_09R Network E	en contr) option ate] (Mineret (Mineret)	Application Version 7.1009-73140 Application Version 7.1009-73140 Application Version	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a Click OK to Click OK to Main Menu: Adminitive Hostname Action Sturit Auto upgrad Sturit Auto upgrad 	de Settings s mated upgrad appropriate I start the upg start the upg	ection of th de. Select SO from the grade. are Manageme Status OAM HA Role Clarify OAM HA Role COAM HA Role	e Initiate Serial m e Upgrae nt -> Upgra Appl HA Role NA Appl HA Role	e scree node. de ISC de [Initia Network E so1_DSR Network E so1_DSR	en contr) option ate] (Mineret (Mineret)	Application Version 7.3000-73140	
18.	VIP: Initiate SBR upgrade	The Upgrad of the autor Select the a Select the a Click OK to Main Menu: Admini Mostanne Action Stats Auto upgrad SER3 Auto upgrad	de Settings s mated upgrad appropriate IS start the upg stration -> Softw	ection of the de. Select SO from the grade. are Manageme Status OAM HA Role Clarify OAM HA Role Select To up Select "Balk" to up	e Initiate Serial m e Upgrad nt -> Upgra Appl HA Role NVA Appl HA Role NVA Appl HA Role NVA ada mode grade servers et despated last se ated according to	e scree node. de ISC de ISC de [Initia Network E so1_DSR Network E so1_DSR Network E so1_DSR Network E	en contr) option ate] iement VM iement VM iement VM iement	Application Version 7,000-73-14.0 Application Version 7,000-73-14.0 Application Version 7,000-73-14.0 Application Version 7,000-73-14.0 Application Version 7,000-73-14.0 Application Version 7,000-73-14.0	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a Click OK to Click OK to Main Menu: Adminitive Hostname Action SUR1 Auto upgrad SBR2 Auto upgrad SBR3 Auto upgrad 	de Settings s mated upgrad appropriate IS start the upg stration -> Softw	ection of the de. Select SO from the grade. are Manageme Status OAM HA Role Dame OAM HA Role Dame Select Total to Select Total total to Select Total total total total total total total total total total t	e Initiate Serial m e Upgrad nt -> Upgra Appl HA Role NA Appl HA Role NA Appl HA Role NA Appl HA Role NA Appl HA Role NA	e scree node. de ISC de ISC de [initia Network E so1_DSR Network E so1_DSR Network E so1_DSR Network E so1_DSR Network E so1_DSR Network E	en contr) option ate] Assess Asse	Application Version 7,000-73-14.0 Application Version 7,000-73-14.0 Application Version 7,000-73-14.0 Application Version 7,000-73-14.0 Application Version 7,000-73-14.0 Application Version 7,000-73-14.0	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a Click OK to Click OK to Main Menu: Admini Info Hostwatte Action SUR1 Auto upgrad SUR1 Auto upgrad SUR3 Auto upgrad 	de Settings s mated upgrad appropriate IS start the upg stration -> Softw	ection of the de. Select SO from the grade. are Manageme Status OAM HA Role Dentily OAM HA Role Dentily Deficit (Cooperative Select The Arose other Deficit (NONE' - all serve	e Initiate Serial m e Upgrad nt -> Upgrad Appl HA Role NVA Appl HA Role NVA Appl HA Role NVA add mode grade servers in g sparade servers of begrade servers of the servers of the servers	e SCREE node. de ISC de ISC de [Initia Network E SC1_DSR, Network E SC1_DSR, Network E SC1_DSR, Network E SC1_DSR, invest of the ini- invest of the ini- screen will be the 'Applicat scion will be	en contr) option ate] Assess Asse	Application Version 7.3000-73.140 Application Version 7.3000-73.140 Application Version 7.3000-73.140 Application Version 7.3000-73.140 ability setting in HA order. g to the availability setting the server.	
18.	VIP: Initiate SBR upgrade	 The Upgrad of the autor Select the a Click OK to Click OK to Main Menu: Admini Info Hostwatte Action SUR1 Auto upgrad SUR1 Auto upgrad SUR3 Auto upgrad 	de Settings s mated upgrad appropriate IS start the upg stration -> Softw	ection of the de. Select SO from the grade. are Manageme Status OAM HA Role Dentily OAM HA Role Dentily Deficit (Cooperative Select The Arose other Deficit (NONE' - all serve	e Initiate Serial m e Upgrad nt -> Upgrad Appl HA Role NVA Appl HA Role NVA Appl HA Role NVA add mode grade servers in g sparade servers of begrade servers of the servers of the servers	e SCREE node. de ISC de ISC de [Initia Network E SC1_DSR, Network E SC1_DSR, Network E SC1_DSR, Network E SC1_DSR, invest of the ini- invest of the ini- screen will be the 'Applicat scion will be	en contr) option ate] Assess Asse	Application Version 7.3000-73.140 Application Version 7.3000-73.140 Application Version 7.3000-73.140 Application Version 7.3000-73.140 ability setting in HA order. g to the availability setting the server.	

Step #	Procedure	Description								
19.	Active NOAM VIP: View the	Observe the U displays under						le status		
	upgrade	Main Menu: Adm	Main Menu: Administration -> Software Management -> Upgrade							
	administration form to monitor	Filter* - Status - Tasks -								
	upgrade	NO_SO SO_East	SO_North SO_Weil							
	progress	Entre Site SO_East	IPFE_SG1 IPFE_SG	2 IPFE_SG3	IPFE_SG4 MP_SG	SBR, SG	\$97_\$G1	897_962		
		Hostname		OAM HA Role Appl HA Role	Server Role Network Element	Function	Application			
		SBR1	Pending	Standby Active	MP SO1_DSR_VM	SBR	7.3.0.0.0-7	3.14.0 0.0_80.20.0×86_64.iso		
		58R2	Pending	Active	MP	SER	7.3.0.0.0-7	Sector And Andrews Sector		
		oona	Nom	Standby	SO1_DSR_VM	SBR	DSR-8,0.0	0.0_80.20.0->86_64.iso		
		SBR3	Upgrading	NA	SO1_DSR_VM	opn		0.0_88.20.0-x86_64.iso		
				-						
21.	each SBR server group Identify the STP server group(s) to	per Table 16. From the data upgrade in iter		Table 16, i	dentify the	STP se	rver gr	oup(s) to		
	upgrade									
22.	Active NOAM	1. Navigate t	o Administra	ation > So	oftware Ma	nagem	ent > l	Jpgrade.		
	VIP : View pre- upgrade status	2. Select the	SOAM tab o	f the site b	eing upgra	ded.				
	of vSTP MP	3. Select the	link for each	vSTP ser	ver group to	o upgra	de.			
	servers		TP servers to lue is the exp					he Application sion.		
		Backup.	is in Backup The Upgrade o is complete	State cha	inges to Ba	ckup ir	n Prog	ress. When		
			OAM Max Ha					ither standby or		
		Main Menu: Adr	ninistration ->	Software M	anagement 🞝	> Upgrad	le			
		Filter • Tasks	•							
		NO_56 50_501								
		Entire Site SO_SG1	SO1MP_SG1							
		-10000000	Upgrade State	OAM HA Ro	e Server Rol	le Fi	unction	Application Version		
		Hostname	Server Status	Appl HA Rol	e Network El	lement				
				200 C 10 C				Upgrade ISO		
		fgtt-so1mp1	Backup Need	100000000000	MP SO_NE1	S	ΓP	8 1.0 0.0-81 17.0		

	Procedure	Description					
23.	Active NOAM VIP: Verify upgrade status	This may take a being upgraded The Upgrade A	d, new alarms	s may occur			-
	is Ready for the server to	server group be			layer nange		
	be upgraded	Main Menu: Adm	inistration -> S	oftware Mana	agement -> Upg	rade	
		Filter" • Tasks •	9. 19				1
		NO_SG SO_SG1					
		Entire Ster SO_SG1	501MP_501				
		Hostname	Upgrade State Server Status	OAM HA Role	Server Role Network Element	Function	Application Version
		E.	Ready	Active	MP	STP	8 1.0.0.0-81 17.0
		fgtt-solimp1	Warm	NA	SO_NE1		1
		Backup Backup All	Checkup Che	ckup All Upgrad	le Server Accept	Report	Report All
		Servers may ha	ave a combin	ation of the	following exp	ected al	arms.
		Alarm	ID = 32515 (Server HA I	Eailovor Inhil	nited)	
		Alarm Alarm Alarm mate h Alarm Alarm	ID = 31101 (ID = 31106 (ID = 31107 (ID = 31228 (heartbeats) o ID = 31114 (ID = 31225 (DB Replica DB Merge t DB Merge F HA Highly a r (Lost Cor DB Replica HA Service	tion to slave o Parent Fail From Child Fa available serv nmunication tion over SO Start Failure	DB has ure) ailure) ver faile with Ma AP has	ed to receive ate Server)
24.	Active NOAM VIP: Initiate vSTP MP upgrade (part 1)	Alarm Alarm Alarm mate h Alarm Alarm Select the Upg 1. From the U upgraded. 2. Click Upgr Main Menu: Adm	ID = 31101 () ID = 31106 () ID = 31107 () ID = 31228 () eartbeats) o ID = 31114 () ID = 31225 () rade Server () opgrade Administration -> S	DB Replica DB Merge t DB Merge F HA Highly a r (Lost Cor DB Replica HA Service	tion to slave o Parent Fail From Child Fa available serv nmunication tion over SO Start Failure thod. creen, select t	DB has ure) ailure) ver faile with Ma AP has e)	ed to receive ate Server) failed)
24.	VIP: Initiate vSTP MP upgrade (part	Alarm Alarm Alarm Marm Alarm Alarm Select the Upg 1. From the U upgraded. 2. Click Upgra	ID = 31101 () ID = 31106 () ID = 31107 () ID = 31228 () eartbeats) o ID = 31114 () ID = 31225 () rade Server () opgrade Administration -> S	DB Replica DB Merge t DB Merge F HA Highly a r (Lost Cor DB Replica HA Service	tion to slave o Parent Fail From Child Fa available serv nmunication tion over SO Start Failure thod. creen, select t	DB has ure) ailure) ver faile with Ma AP has e)	ed to receive ate Server) failed)
24.	VIP: Initiate vSTP MP upgrade (part	Alarm Alarm Alarm mate h Alarm Alarm Select the Upg 1. From the U upgraded. 2. Click Upgr Main Menu: Adm	ID = 31101 () ID = 31106 () ID = 31107 () ID = 31228 () eartbeats) o ID = 31114 () ID = 31225 () rade Server () opgrade Administration -> S	DB Replica DB Merge t DB Merge F HA Highly a r (Lost Cor DB Replica HA Service	tion to slave o Parent Fail From Child Fa available serv nmunication tion over SO Start Failure thod. creen, select t	DB has ure) ailure) ver faile with Ma AP has e)	ed to receive ate Server) failed)
24.	VIP: Initiate vSTP MP upgrade (part	Alarm Alarm Alarm mate h Alarm Alarm Select the Upg 1. From the U upgraded. 2. Click Upgr Main Menu: Adm	ID = 31101 () ID = 31106 () ID = 31107 () ID = 31228 () eartbeats) o ID = 31114 () ID = 31225 () rade Server () opgrade Administration -> S	DB Replica DB Merge t DB Merge F HA Highly a r (Lost Cor DB Replica HA Service	tion to slave o Parent Fail From Child Fa available serv nmunication tion over SO Start Failure thod. creen, select t	DB has ure) ailure) ver faile with Ma AP has e)	ed to receive ate Server) failed)
24.	VIP: Initiate vSTP MP upgrade (part	Alarm Alarm Alarm Alarm Alarm Alarm Select the Upg 1. From the U upgraded. 2. Click Upgr Main Menu: Adm Flitter Tasks	ID = 31101 ((ID = 31106 () ID = 31107 () ID = 31228 () eartbeats) o ID = 31114 () ID = 31225 () rade Server () lpgrade Admi ade Server.	DB Replica DB Merge t DB Merge F HA Highly a r (Lost Cor DB Replica HA Service	tion to slave o Parent Fail From Child Fa available serv nmunication tion over SO Start Failure thod. creen, select t	DB has ure) ailure) ver faile with Ma AP has e)	ed to receive ate Server) failed)
24.	VIP: Initiate vSTP MP upgrade (part	Alarm Alarm Alarm Alarm Alarm Alarm Select the Upg 1. From the U upgraded. 2. Click Upgr Main Menu: Adm Filter Tasks	ID = 31101 () ID = 31106 () ID = 31107 () ID = 31228 () eartbeats) o ID = 31114 () ID = 31225 () rade Server () pgrade Admi ade Server. inistration -> S <u>SOIMP_SG1</u> Upgrade State Server Status	DB Replica DB Merge to DB Merge F HA Highly a r (Lost Cor DB Replica HA Service upgrade met inistration so Software Mana	tion to slave o Parent Fail From Child Fa available servin munication tion over SO Start Failure thod. creen, select to agement -> Upg	DB has ure) ailure) ver faile with Ma AP has) he serve rade	ed to receive ate Server) failed) er to be Application Version Upgrade 150
24.	VIP: Initiate vSTP MP upgrade (part	Alarm Alarm Alarm Alarm Alarm Alarm Select the Upg 1. From the U upgraded. 2. Click Upgr Main Menu: Adm Flitter Tasks	ID = 31101 () ID = 31106 () ID = 31107 () ID = 31228 () eartbeats) o ID = 31124 () ID = 31225 () rade Server () pgrade Administration -> S <u>SOIMP_SG1</u> Upgrade State Server Status Plendy	DB Replica DB Merge to DB Merge F HA Highly a r (Lost Cor DB Replica HA Service upgrade met inistration so Goftware Mana	tion to slave o Parent Fail From Child Fa available served nmunication tion over SO Start Failure thod. creen, select to agement -> Upg	DB has ure) ailure) ver faile with Ma AP has e) he serve	ed to receive ate Server) failed) er to be
24.	VIP: Initiate vSTP MP upgrade (part	Alarm Alarm Alarm Alarm Alarm Alarm Select the Upg 1. From the U upgraded. 2. Click Upgr Main Menu: Adm Filter Tasks • NO_SG SO_SG1 Entire Ster SO_SG1 Hostname	ID = 31101 () ID = 31106 () ID = 31107 () ID = 31228 () eartbeats) o ID = 31225 () ID = 31225 () rade Server () pgrade Admi ade Server. inistration -> S <u>SOIMP_SG1</u> Upgrade State Server Status <u>Ready</u> <u>Vaim</u>	DB Replica DB Merge to DB Merge F HA Highly a r (Lost Cor DB Replica HA Service upgrade met inistration so Software Mana	tion to slave o Parent Fail From Child Fa available server nmunication tion over SO Start Failure thod. creen, select to agement -> Upg	DB has ure) ailure) ver faile with Ma AP has) he serve rade	ed to receive ate Server) failed) er to be Application Version Upgrade 150

Step #	Procedure	Description
25.	Active NOAM VIP: Initiate vSTP upgrade (part 2)	Select target ISO. 1. On the Upgrade Initiate screen, select the target ISO from the Upgrade ISO options. 2. Click OK to initiate the upgrade. Main Menu: Administration -> Software Management -> Upgrade [Initiate] Info® Hostname Action Status Action Status Upgrade Settings Upgrade Settings Upgrade ISO DSR-8.1.0.0.0_81.18.0-x86_64.150 Select the desired upgrade ISO media file
26.	Active NOAM VIP: View the upgrade administration form to monitor upgrade progress	Ok Cancel Observe the Upgrade State of the vSTP MP server. Upgrade status displays under the Status Message column. Main Menu: Administration -> Software Management -> Upgrade Filter* Tasks * NO. 50_562 SO_563 Filter* Tasks * MO. 50_562 SO_563 Filter* Tasks * MO. 50_563 SO_563 Filter* Tasks * Mo. 50_563 SO_563 Filter* Tasks * Mo. 50_563 SO_563 Filter* Tasks * Mo. So_563 SO_563 Filter* Tasks * Upgrade State Upgrade State OAM HA Role Not SO_NET Upgrade ISO Steedby Mo. SO_NET OSR 81000_6t 190-680_64 inp
27.	Repeat for each vSTP server(s).	Repeat steps 22. through 26. for the next vSTP servers to be upgraded per Table 16.
28.	Active NOAM VIP: View the upgrade administration form to monitor upgrade progress	 See step 29. for instructions if the upgrade fails, or if execution time exceeds 60 minutes. <i>Note</i>: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as FAILED. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Sequence through the server group links for the server groups being upgraded. Observe the Upgrade State of the servers of interest. Upgrade status displays under the Status Message column. During the upgrade, the servers may have a combination of the following expected alarms.

Step #	Procedure	Description
		<i>Note</i> : Not all servers have all alarms:
		Alarm ID = 10008 (Provisioning Manually Disabled)
		Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)
		Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)
		Alarm ID = 31101 (DB Replication To Slave Failure)
		Alarm ID = 31106 (DB Merge To Parent Failure)
		Alarm ID = 31107 (DB Merge From Child Failure)
		Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)
		Alarm ID = 31233 (HA Secondary Path Down)
		Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)
		Alarm ID = 32515 (Server HA Failover Inhibited)
		Alarm ID = 31114 (DB Replication over SOAP has failed)
		Alarm ID = 31225 (HA Service Start Failure)
		Database (DB) replication failure alarms may display during an Automated Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved. Refer to Appendix O resolve this issue.
		 Half of the DA-MP and SBR server groups are upgraded in iteration 3. ASG automatically sequences to iteration 4 to upgrade the remaining servers. Periodically monitor these servers for failures.
		 For the IPFE servers being upgraded, wait for the upgrades to complete. The Status Message column displays Success after approximately 20 to 50 minutes. Do not proceed to iteration 4 until the IPFE servers have completed upgrade.
		<i>Note</i> : Do not accept any upgrades at this time.
		If any upgrade fails – do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix I for failed server recovery procedures.
29.	Server CLI: If the upgrade of	If the upgrade of a server fails, access the server command line (using ssh or a console), and collect the following files:
	a server fails	/var/TKLC/log/upgrade/upgrade.log
		/var/TKLC/log/upgrade/ugwrap.log
		/var/TKLC/log/upgrade/earlyChecks.log
		/var/TKLC/log/platcfg/upgrade.log
		It is recommended to contact My Oracle Support (MOS) and provide these files. Refer to Appendix I for failed server recovery procedures.

5.3.5 Upgrade Iteration 4

Upgrade iteration 4 continues the upgrade of the site C-level servers. As shown in Table 16, iteration 4 consists of upgrading the second half of the DA-MPs, vSTPs, and IPFEs, as well as the standby SBR(s), if equipped.

Table 20 shows the estimated time required to upgrade the C-level servers for iteration 4.

 Table 20. Iteration 4 Upgrade Execution Overview.

	Elapsed Time (hr:min)		Procedure	
Procedure	This Step	Cum.	Title	Impact
Procedure 25	0:40-1:00	0:40-1:00	Procedure 25	1/2 DA-MPs, 1/2 IPFEs, standby SBR(s), 1/2 vSTP servers are offline

Procedure 25 provides the steps to upgrade, $\frac{1}{2}$ of the vSTPs servers and $\frac{1}{2}$ of the IPFEs. ASG automatically upgrades the DA-MPs and SBRs.

Procedure 25. Upgrade Iteration 4

Step #	Procedure	Description					
Check o number.	off $()$ each step as	a portion of the C-level servers for iteration 4. it is completed. Boxes have been provided for this purpose under each step recommended to contact My Oracle Support (MOS) and ask for assistance.					
1.	Identify the IPFE server group(s) to upgrade	From the data captured in Table 16, identify the IPFE server group(s) to upgrade in iteration 4.					
2.	Active NOAM VIP: View pre- upgrade status of IPFEs	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being upgraded. Select the link of each IPFE server group to be upgraded. For the IPFE servers to be upgraded in iteration 4, verify the application 					
		 version value is the expected source software release version. 5. If a server is in Backup Needed state, select the servers and click Backup. The Upgrade State changes to Backup in Progress. When the backup is complete, the Upgrade State changes to Ready. 6. Verify the OAM Max HA Role is in the expected condition (either standb or active). This depends on the server being upgraded. 					
		Main Menu: Administration -> Software Management -> Upgrade Filter* Tasks • N0_90 S0_East 80_North S0_West Entire Site S0_East IPFE_SG1 IPFE_SG3 IPFE_SG3 S8R_SG SS7_SG1 SS7_S					

Procedure	Description
Active NOAM VIP: Verify upgrade status is Ready for	This may take a minute if a backup is in progress. Depending on the server being upgraded, new alarms may occur. The Upgrade Administration screen displays. Navigate to the IPFE server group being upgraded.
the server to	Main Menu: Administration -> Software Management -> Upgrade
be upgraded	Filter* Tasks NO_SG SO_Eant SO_Eant SO_North SO_Eant SO_West Entire Site SO_East IPFE_SQ2 IPFE_SQ3 IPFE_SQ4 MP_SQ SBR_SQ SS7_SQ1
	Hostname Upgrade State OAM HA Role Server Role Function Application Version Server Status Appl HA Role Network Element Upgrade ISO IPFE1 Ready Active MP IP Front End 7.3.0.0.9-73.18.0
	Servers may have a combination of the following expected alarms. Note: Not all servers have all alarms: Alarm ID = 10008 (Provisioning Manually Disabled) Alarm ID = 10073 (Server Group Max Allowed HA Role Warning) Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped) Alarm ID = 32515 (Server HA Failover Inhibited) Alarm ID = 31101 (DB Replication to slave DB has failed) Alarm ID = 31106 (DB Merge to Parent Failure) Alarm ID = 31107 (DB Merge From Child Failure) Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server) Alarm ID = 31114 (DB Replication over SOAP has failed) Alarm ID = 31225 (HA Service Start Failure)
Active NOAM VIP: Initiate IPFE upgrade (part 1)	 Select the Upgrade Server method. 1. From the Upgrade Administration screen, select the server to be upgraded. 2. Click Upgrade Server. Main Menu: Administration -> Software Management -> Upgrade Filter* Tasks *
	VIP: Verify upgrade status is Ready for the server to be upgraded

Step #	Procedure	Description					
5.	Active NOAM VIP: Initiate IPFE upgrade (part 2)	 Select target ISO. 1. On the Upgrade Initiate screen, select the target ISO from the Upgrade ISO options. 2. Click OK to initiate the upgrade. Main Menu: Administration -> Software Management -> Upgrade [Initiate]					
		Hostname Action	Status				
		IPFE1 Upgrade	OAM HA Role	Appl HA Role N/A	Network Element SO1_DSR_VM		
		Upgrade Settings					
		Upgrade ISO DSR-8.0.0.0_80.20.0-x86_64.iso V Ok Cancel	Select the desired	l upgrade ISO med	lia file.		
6.	Active NOAM VIP: View the upgrade administration form to monitor upgrade progress	Observe the Upgrade State of the IPF under the Status Message column. Main Menu: Administration -> Software Man Filter • Status • Tasks • IPFE_SG_MP_SG_ND_SG_SO_SG Hostname Upgrade State Status • Appl Max HA Role Upgrade State Upgrade State Standby OOS	nagement -> (Server Role F Network Element	Upgrade unction Applicat Upgrade	tion Version ± 150		
7 .	Repeat for each IPFE	Repeat steps 1. through 6. for the nex	t IPFE to be	upgraded	per Table 16.		
8.	Server CLI: If the upgrade of a server fails:	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files: /var/TKLC/log/upgrade/upgrade.log /var/TKLC/log/upgrade/ugwrap.log /var/TKLC/log/upgrade/earlyChecks.log /var/TKLC/log/platcfg/upgrade.log If any upgrade fails – do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix I for failed server recovery procedures.					
9. □	Identify the STP server group(s) to upgrade	From the data captured in Table 16, ic upgrade in iteration 4.	lentify the S	TP server ç	group(s) to		

Step #	Procedure	Description					
10.	Active NOAM	1. Navigate to	Administrati	on > Softv	ware Manage	ment >	Upgrade.
	VIP: View pre- upgrade status	2. Select the S	SOAM tab of the	ne site beir	ng upgraded.		
	of vSTP MP	3. Select the li	nk for each vS	STP server	group to upg	rade.	
	servers		P servers to b ue is the expe				the Application
		Backup. T the backup 6. Verify the C	is complete, the state of the s	tate chang he Upgrade Role is the the server	es to Backup e State chang expected cor being upgrad	o in Prog ges to R ndition (e ded.	gress. When
		Filter* • Tasks • NO_SG SO_SG1 Entire Site SO_SG1	SO1MP_SG1				
		Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
		(Contraine	Server Status	Appl HA Role	Network Element		
			states which is a set of second states on the local second				Upgrade ISO
		fatt-so1mp1	Backup Needed	Active	MP	STP	Upgrade ISO 8 1 0 0 0-81 17 0

Step #	Procedure	Description					
11. □	Active NOAM VIP: Verify upgrade status	This may take a being upgraded The Upgrade A	, new alarms	s may occur.		•	
	is Ready for the server to	server group be	ing upgrade	d.			
	be upgraded	Main Menu: Admi	nistration -> S	oftware Mana	igement -> Upg	jrade	
		Filter" • Tasks •					
		NO_SG SO_SG1					
		Entire Ster SO_SG1	SO1MP_SG1 Upgrade State	OAM HA Role	Server Role	Function	Application Version
		1	Server Status	Appl HA Role	Network Element	1	Upgrade ISO
		fgtt-so.tmp1	Ready Warm	Active N/A	SO_NE1	STP	8 10.0.0-81.17.0
		Backup Backup All	Checkup Che		e Server) Accept	Report	Report All
		Servers may ha	ve a combin	ation of the	following exp	actad a	larms
		Alarm I Alarm I becaus	D = 10073 (D = 10075 (e applicatio	The server	up Max Allov is no longer	ved HA providi manua	Role Warning) ing services ally stopped)
		Alarm I Alarm I becaus Alarm I Alarm I Alarm I Alarm I Alarm I	D = 10073 (3) $D = 10075 (7)$ $D = 32515 (3)$ $D = 31101 (1)$ $D = 31106 (1)$ $D = 31107 (1)$ $D = 31228 (1)$	Server Grou The server on processe Server HA F DB Replicat DB Merge to DB Merge F HA Highly a	up Max Allov is no longer s have been Failover Inhil tion to slave o Parent Fail From Child F	ved HA providi manua bited) DB has ure) ailure) ver faile	Role Warning) ing services ally stopped) s failed) ed to receive
12.	Active NOAM VIP: Initiate vSTP MP upgrade (part 1)	Alarm I Alarm I becaus Alarm I Alarm I Alarm I Alarm I Alarm I Select the Upgr 1. From the Up upgraded. 2. Click Upgra	D = 10073 (D = 10075 (D = 32515 (D = 31101 (D = 31106 (D = 31106 (D = 31228 (eartbeats) o ade Server u pgrade Adminie	Server Grou The server on processe Server HA F DB Replicat DB Merge f DB Merge F HA Highly a rr (Lost Con upgrade met inistration sc	up Max Allov is no longer s have been Failover Inhil tion to slave o Parent Fail From Child Fa available serv nmunication thod. creen, select t	ved HA providi manua bited) DB has ure) ailure) ver faile with M	Role Warning) ing services ally stopped) s failed) ed to receive late Server)
12.	VIP: Initiate vSTP MP upgrade (part	Alarm I Alarm I becaus Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Select the Upgr 1. From the Uj upgraded. 2. Click Upgra Main Menu: Admi	D = 10073 (D = 10075 (D = 32515 (D = 31101 (D = 31106 (D = 31106 (D = 31228 (eartbeats) o ade Server u pgrade Adminie	Server Grou The server on processe Server HA F DB Replicat DB Merge f DB Merge F HA Highly a rr (Lost Con upgrade met inistration sc	up Max Allov is no longer s have been Failover Inhil tion to slave o Parent Fail From Child Fa available serv nmunication thod. creen, select t	ved HA providi manua bited) DB has ure) ailure) ver faile with M	Role Warning) ing services ally stopped) s failed) ed to receive late Server)
12.	VIP: Initiate vSTP MP upgrade (part	Alarm I Alarm I becaus Alarm I Alarm I Alarm I Alarm I Alarm I Select the Upgr 1. From the Up upgraded. 2. Click Upgra	D = 10073 (D = 10075 (D = 32515 (D = 31101 (D = 31106 (D = 31106 (D = 31228 (eartbeats) o ade Server u pgrade Adminie	Server Grou The server on processe Server HA F DB Replicat DB Merge f DB Merge F HA Highly a rr (Lost Con upgrade met inistration sc	up Max Allov is no longer s have been Failover Inhil tion to slave o Parent Fail From Child Fa available serv nmunication thod. creen, select t	ved HA providi manua bited) DB has ure) ailure) ver faile with M	Role Warning) ing services ally stopped) s failed) ed to receive late Server)
12.	VIP: Initiate vSTP MP upgrade (part	Alarm I Alarm I becaus Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Select the Upgr 1. From the Uj upgraded. 2. Click Upgra Main Menu: Admi	D = 10073 (D = 10075 (D = 32515 (D = 31101 (D = 31106 (D = 31106 (D = 31228 (eartbeats) o ade Server u pgrade Adminie	Server Grou The server on processe Server HA F DB Replicat DB Merge f DB Merge F HA Highly a rr (Lost Con upgrade met inistration sc	up Max Allov is no longer s have been Failover Inhil tion to slave o Parent Fail From Child Fa available serv nmunication thod. creen, select t	ved HA providi manua bited) DB has ure) ailure) ver faile with M	Role Warning) ing services ally stopped) s failed) ed to receive late Server)
12.	VIP: Initiate vSTP MP upgrade (part	Alarm I Alarm I becaus Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Select the Upgr 1. From the Uj upgraded. 2. Click Upgra Main Menu: Admi	D = 10073 (D = 10075 (D = 32515 (D = 31101 (D = 31106 (D = 31106 (D = 31228 (eartbeats) o ade Server u pgrade Adminie	Server Grou The server on processe Server HA F DB Replicat DB Merge f DB Merge F HA Highly a rr (Lost Con upgrade met inistration sc	up Max Allov is no longer s have been Failover Inhil tion to slave o Parent Fail From Child Fa available serv nmunication thod. creen, select t	ved HA providi manua bited) DB has ure) ailure) ver faile with M	Role Warning) ing services ally stopped) s failed) ed to receive late Server)
12.	VIP: Initiate vSTP MP upgrade (part	Alarm I Alarm I becaus Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Select the Upgr 1. From the Up upgraded. 2. Click Upgra Main Menu: Admi	D = 10073 ($\frac{1}{2}$ D = 10075 ($\frac{1}{2}$ D = 32515 ($\frac{1}{2}$ D = 31101 ($\frac{1}{2}$ D = 31106 ($\frac{1}{2}$ D = 31107 ($\frac{1}{2}$ D = 31228 ($\frac{1}{2}$ eartbeats) o ade Server upgrade Admini- ade Server.	Server Grou The server on processes Server HA F DB Replicat DB Merge for DB Merge F HA Highly a r (Lost Con upgrade met inistration sc Software Mana	up Max Allov is no longer s have been Failover Inhil tion to slave o Parent Fail From Child Fa available serv nmunication thod. creen, select t	ved HA providi manua bited) DB has ure) ailure) ver faile with M	Role Warning) ing services ally stopped) s failed) ed to receive late Server) er to be
12.	VIP: Initiate vSTP MP upgrade (part	Alarm I Alarm I becaus Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Select the Upgr 1. From the Up upgraded. 2. Click Upgra Main Menu: Admi Filter Tasks • No.33 50_531	D = 10073 ($\frac{1}{2}$ D = 10075 ($\frac{1}{2}$ D = 10075 ($\frac{1}{2}$ D = 10075 ($\frac{1}{2}$ D = 32515 ($\frac{1}{2}$ D = 31107 ($\frac{1}{2}$ D = 31106 ($\frac{1}{2}$ D = 31107 ($\frac{1}{2}$ D = 31228 ($\frac{1}{2}$ D = 3128 ($\frac{1}{2}$ D = 3	Server Grou The server on processes Server HA F DB Replicat DB Merge to DB Merge to DB Merge F HA Highly a r (Lost Con upgrade met inistration sc Software Mana	up Max Allov is no longer es have been Failover Inhil tion to slave o Parent Fail from Child Fa available sern nmunication thod. creen, select to agement -> Upg	ved HA providi manua bited) DB has ure) ailure) ver faile with M the serv	Role Warning) ing services ally stopped) is failed) ed to receive late Server) err to be
12.	VIP: Initiate vSTP MP upgrade (part	Alarm I Alarm I becaus Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Alarm I Select the Upgr 1. From the Up upgraded. 2. Click Upgra Main Menu: Admi Filter Tasks • No.33 50_531	D = 10073 ($\frac{1}{2}$ D = 10075 ($\frac{1}{2}$ D = 3075 ($\frac{1}{2}$ D = 31101 ($\frac{1}{2}$ D = 31106 ($\frac{1}{2}$ D = 31106 ($\frac{1}{2}$ D = 31107 ($\frac{1}{2}$ D = 31228 ($\frac{1}{2}$ eartbeats) of ade Server up grade Administration -> S	Server Grou The server on processes Server HA F DB Replicat DB Merge for DB Merge F HA Highly a r (Lost Con upgrade met inistration sc Software Mana	up Max Allov is no longer es have been Failover Inhil tion to slave o Parent Fail From Child Fa available sern nmunication thod. creen, select to agement -> Upg	ved HA providi manua bited) DB has ure) ailure) ver faile with M	Role Warning) ing services ally stopped) is failed) ed to receive ate Server) er to be

Step #	Procedure	Description						
13.	Active NOAM VIP: Initiate vSTP upgrade (part 2)	 Select target ISO. 1. On the Upgrade Initiate screen, select the target ISO from the Upgrade ISO options. 2. Click OK to initiate the upgrade. Main Menu: Administration -> Software Management -> Upgrade [Initiate] 						
		Hostname	Action		Status			
		fgtl-so1mp1	Upgrade		OAM HA Role	Appi HA	Role Network Element	
		Upgrade Settings Upgrade ISO Ok Cancel	DSR-8.1.0.0.0_81.1	8.0-x86_64.iso	 Select the desired u 	pgrade ISO me	edia file	
14.	Active NOAM VIP: View the upgrade administration form to monitor upgrade progress	under the Sta	tus Message ministration -> S • so_soz so_soz	column.			rade status displays	
		Hostname	Upgrade State	QAM HA Role	Server Role	Function	Application Version	
			Server Status	Appl HA Role	Network Element		Upgrade ISO	
		fgtt-so1mp1	Upgrading	Standby	SO_NE1	STP	8.1.0.0.0-81.17.0 DSR-8.1.0.0.0_81.18.0.x88_64.iss	
15.	Repeat for each vSTP server(s).	Repeat steps Table 16.	10. through 7	14. for the r	next vSTP se	ervers to	be upgraded per	
16.	Identify the Standby SBR server(s) to upgrade	iteration 4. If ASG was us already upgra If a manual up	sed in Upgrad aded and this ograde was re	de Iteration step is not ecommend	3, then the required.	standby alternate	ver (s) to upgrade in SBR server(s) is e upgrade erver (s) upgrade.	

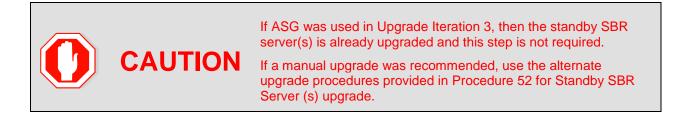
5.3.6 Upgrade Iteration 5

Upgrade iteration 5 continues the upgrade of the site C-level servers. As shown in Table 16, iteration 5 consists of upgrading the active SBR(s).

Table 21 shows the estimated time required to upgrade the remaining C-level servers for iteration 5.

 Table 21. Iteration 5 Upgrade Execution Overview

	Elapsed Time (hr:min) Procedure This Step			
Procedure			Procedure Title	Impact
Procedure 26	0:40-1:00	0:40-1:00	Procedure 26	Standby SBR becomes active; previously active SBR is offline for upgrade



Procedure 26. Upgrade Iteration 5

Step #	Procedure	Description					
This proc	edure upgrades	the active SBRs					
				e been pro	ovided for th	is purpo	ose under each step
f this pro	ocedure fails, it is	recommended t	o contact My	/ Oracle S	upport (MOS	S) and a	ask for assistance.
1.	Active NOAM VIP: Iteration	active.				_	standby to become
	5	Main Menu: Admi	inistration -> So	ftware Mana	gement -> Upgr	ade	
		Filter* + Status +	Tasks +				
		NO_SO SO East	50_North SO_West				
		Entre Site SO_East	IPFE_SG1 IPFE_S	G2 IPFE_963	IPFE_SG4 MP_SG	SBR_SG	887_961 887_962
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO
		SER1	Accept or Reject	Active	MP	SBR	8 0 0 0 0 80 20 0
		SON I	Err	Active	SO1_DSR_VM		DSR-8.0.0.0.0_80.20.0or86_64 iso
		58R2	Upgrading	005	MP	SBR	7.3.0.0.0-73.14.0
			Unk	N/A	SO1_DSR_VM		DSR-8.0.0.0.0_80.20.0-x86_64.iso
		SBR3	Accept or Reject	Spare	MP	SBR	8.0.0.0 80.20.0
		10000	En	Spare	SO1_DSR_VM		DSR-8.0.0.0.0_80.20.0-x85_54.iso
						.,	
2.	Active NOAM VIP: View the upgrade administration	See step 3 for minutes.	Instructions	if the upg	rade fails, or	it exec	ution time exceeds 6

Step #	Procedure	Description
	form to monitor upgrade	Note: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as FAILED .
	progress	The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem.
		1. Navigate to Administration > Software Management > Upgrade.
		2. Select the SOAM tab of the site being upgraded.
		 Sequence through the server group links for the server groups being upgraded. Observe the upgrade state of the servers of interest. Upgrade status displays under the Status Message column.
		During the upgrade, the servers may have a combination of the following expected alarms.
		Note: Not all servers have all alarms:
		Alarm ID = 10008 (Provisioning Manually Disabled)
		Alarm ID = 10073 (Server Group Max Allowed HA Role Warning)
		Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped)
		Alarm ID = 31101 (DB Replication To Slave Failure)
		Alarm ID = 31106 (DB Merge To Parent Failure)
		Alarm ID = 31107 (DB Merge From Child Failure)
		Alarm ID = 31228 (HA Highly available server failed to receive mate heartbeats) or (Lost Communication with Mate Server)
		Alarm ID = 31233 (HA Secondary Path Down)
		Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)
		Alarm ID = 32515 (Server HA Failover Inhibited)
		Alarm ID = 31114 (DB Replication over SOAP has failed)
		Alarm ID = 31225 (HA Service Start Failure)
		Database (DB) replication failure alarms may display during an Automated Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved. Refer to Appendix O to resolve this issue.
		Wait for the SBR upgrades to complete. The Status Message column displays Success . This step takes approximately 20 to 50 minutes.
3.	Server CLI: If the upgrade of	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
	a server fails:	/var/TKLC/log/upgrade/upgrade.log
		/var/TKLC/log/upgrade/ugwrap.log
		/var/TKLC/log/upgrade/earlyChecks.log
		/var/TKLC/log/platcfg/upgrade.log
		If any upgrade fails – do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix I for failed server recovery procedures.

5.4 Site Post-Upgrade Procedures



• Procedure 28 Site Post-Upgrade Health Check



After all SOAM sites in the topology have completed upgrade, the upgrade may be accepted using the following procedure:

• Procedure 40 Accept Upgrade

The post-upgrade procedures consist of procedures that are performed after all of the site upgrades are complete. The final Health Check of the system collects alarm and status information to verify that the upgrade did not degrade system operation. After an appropriate soak time, the upgrade is accepted.

5.4.1 Allow Site Provisioning

This procedure enables Site Provisioning for the site just upgraded.



Procedure 27. Allow Site Provisioning

Step #	Procedure	Description				
This pro	This procedure allows provisioning for SOAM and MP servers.					
Check o number.	• • •	it is completed. Boxes have been provided for this purpose under each step				
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	Active SOAM	1. Log into the SOAM GUI of the site just upgraded using the VIP.				
	VIP: Enable site	2. Navigate to Status & Manage > Database.				
	provisioning	3. Click Enable Site Provisioning.				
		4. Confirm the operation by clicking OK on the screen.				
1		5. Verify the button text changes to Disable Site Provisioning .				

5.4.2 Site Post-Upgrade Health Checks

This section provides procedures to verify the validity and health of the site upgrade.

5.4.2.1 Site Post-Upgrade Health Check

This procedure determines the validity of the upgrade, as well as the health and status of the network and servers.

If the **10054 - Device Deployment Failed** alarm displays after the upgrade for any server, see for Appendix S Workaround to Resolve Device Deployment Failed Alarm corrective steps.

Note: If syscheck fails on any server during pre-upgrade checks or in early checks stating that **cpu: FAILURE:** No record in alarm table for FAILURE!, see Procedure 68.

Procedure 28. Site Post-Upgrade Health Check

	Procedure	Description					
-	ocedure verifies pos off (√) each step as			been prov	vided for this p	urpose under ea	ch step
number	· · ·						
If this p	rocedure fails, it is r	ecommended to	o contact My C	Dracle Su	pport (MOS) a	nd ask for assist	ance.
1. Active NOAM VIP: Run automated post- upgrade health checks		 Select the Select the Select the 	SOAM tab of SOAM serve active SOAN	the site r group li I.	being upgrade	being upgraded.	ide.
				tware Mana	gement -> Upgrad	0	
		Eank BNDING_SG		50 55 STXA	MP_SG GTXA_NO_SG	GTXA SESSION SG GTM	50_50
		Hostname	Upgrade State	OAM HA Role Appl HA Role		Application Version Upgrade ISO	
		GTXA-SO1	Accept or Reject	Active NIA	System CAM CA GTXA_1111101_90	M 50000-60.130 DSR-60.000_60.13	0-186 64 180
		GTXA-SO-SP	Accept or Reject	Standby	System CAM CA GTXA_1111101_SO	************************	
		Rectup Backup A	Checkup beckup A	a Upprate Se	Accept Report	Report All	
		7. Click OK. Control r	alth check opt	Upgrade		ade. nt -> Upgrade [C	heckup]
		6. Under He 7. Click OK. Control r Main Menu: /	alth check opt	Upgrade	e screen.		heckup]
		6. Under He 7. Click OK. Control r Main Menu: A Hostname Ac	alth check opt eturns to the Administration	Upgrade	e screen. are Manageme		Аррі
		6. Under He 7. Click OK. Control r Main Menu: A Hostname Ac	alth check opt eturns to the Administration	Upgrade	Status OAM HA Role	nt -> Upgrade [C	Apple
		6. Under He 7. Click OK. Control r Main Menu: A Hostname Ac GTXA.SO1 H Health check options Checkup Type	alth check opt eturns to the Administration	Upgrade	Status OAM HA Role	nt -> Upgrade [C Network Element 07KA_1111101_S0	Аррі
		6. Under He 7. Click OK. Control r Main Menu: A Hostname Ac GTXA SO1 H Health check options Checkup Type	alth check opt eturns to the Administration tion ealth Check Advance Upgrade Phe Upgrade	Upgrade	e Screen. are Manageme Status GAM HA Role Active	Network Element 07XA_1111101_S0	heckup]

Step #	Procedure	Description			
2.	Active NOAM VIP: Monitor health check progress for completion	 Click the Tasks option to display the currently executing tasks. The Health Check task name appears as <soservergroup> PostUpgrade Health Check.</soservergroup> 			
		 Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. 			
		3. Click the hyperlink to download the Health Check report.			
		4. Open the report and review the results.			
		Main Menu: Administration -> Software Management -> Upgrade			
		Filter" - Status - Tasks			
		BarA_BIND/ND_SD ID Hostname Name Task State Details Progress			
		Hostname et 0TXA-NOT Post.gorade Health completed TXA_30_9.0 mm			
		07XA-SO1 45 GTXA-ND1 Ubgrade on completed completed completed completed completed completed completed complete.			
		GTXA-BO-SP (TTXA-Session1 Server +			
3.	Active NOAM VIP: Analyze health check	Analyze Health Check failure. If the Health Check report status is anything other than "Pass", the Health Check logs can be analyzed to determine if the upgrade can proceed.			
	results	1. Navigate to Status & Manage > Files.			
		2. Select the active SOAM tab.			
		3. Select the UpgradeHealthCheck.log file and click View .			
		4. Locate the log entries for the most recent health check.			
		Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact My Oracle Support (MOS) for guidance.			
		If the health check log contains the Unable to execute Health Check on <active hostname="" noam=""></active> message, perform the health checks in Procedure 29.			
4.	Active SOAM	1. Navigate to Diameter Common > Export .			
	VIP : Export and archive the Diameter configuration data	Capture and archive the Diameter data by selecting the ALL option for the Export Application.			
		3. Verify the requested data is exported by clicking Tasks at the top of the screen.			
		 Navigate to Status & Manage > Files and download all the exported files to the client machine, or use the SCP utility to download the files from the active NOAM to the client machine. 			
		5. Navigate to Diameter > Maintenance > Applications .			
	1				

Step #	Procedure	Description
5.	Active SOAM Server: Check if the setup previously has a customer supplied Apache certificate installed and protected with a passphrase, which was renamed before starting with upgrade	If the setup had a customer-supplied Apache certificate installed and protected with passphrase before the start of the upgrade (refer to Procedure 3 and rename the certificate back to the original name.
6.	Compare data to the pre- upgrade health check to verify if the system has degraded after the second maintenance window	Verify that the health check status of the upgraded site as collected from Steps 1 through 4 is the same as the pre-upgrade health checks taken in Section 5.1.2. If system operation is degraded, it is recommended to contact My Oracle Support (MOS).

5.4.2.2 Alternate SOAM Post-Upgrade Health Check

This procedure determines the validity of the upgrade, as well as the health and status of the network and servers. This procedure is an alternative to the normal post upgrade health check in Procedure 30.

Procedure 29. Alternate SOAM Post-Upgrade Health Check

Step #	Procedure	De	scription		
-	This procedure verifies post-upgrade site status. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
If this pr	f this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	Active SOAM	1.	Use an SSH client to connect to the active SOAM:		
	CLI: Run/verify SOAM post-		ssh admusr@ <soam address="" ip="" xmi=""></soam>		
	upgrade health		password: <enter password=""></enter>		
	check status		Note: The static XMI IP address for each server should be available in Table 5.		
		2.	Enter the command:		
			<pre>\$ upgradeHealthCheck postUpgradeHealthCheckOnSoam</pre>		
			This command creates two files in /var/TKLC/db/filemgmt/ UpgradeHealthCheck/ with the filename format:		
			<soserver_name>_ServerStatusReport_<date-time>.xml</date-time></soserver_name>		
			<soserver_name>_ComAgentConnStatusReport_<date- time>.xml</date- </soserver_name>		
			If any alarms are present in the system:		
			<soserver_name>_AlarmStatusReport_<date-time>.xml</date-time></soserver_name>		
			If the system is PDRA, one additional file is generated:		
			<soserver_name>_SBRStatusReport_<date-time>.xml</date-time></soserver_name>		
			<i>Note</i> : The FIPS integrity verification test failed message may display when the upgradeHealthCheck command runs. This message can be ignored.		
		3.	If the Server <hostname> needs operator attention before upgrade message displays, inspect the Server Status Report to determine the reason for the message. If the Server <hostname> has no alarm with DB State as Normal and Process state as Kill message displays in the Server Status Report, the alert can be ignored.</hostname></hostname>		
		No	te: If any server status is not as expected, do not proceed with the upgrade. It is recommended to contact My Oracle Support (MOS) for guidance.		
		4.	Keep these reports for future reference. These reports are compared to alarm and status reports after the upgrade is complete.		

Step #	Procedure	Description	
2.	Active SOAM CLI: Capture Diameter maintenance status	Enter the command: \$ upgradeHealthCheck diameterMaintStatus This command displays a series of messages providing Diameter Maintenance status. Capture this output and save for later use. Note: The output is also captured in /var/TKLC/db/filemgmt/UpgradeHealthCheck.log.	
		Note: The FIPS integrity verification test failed message may display when the upgradeHealthCheck command runs. This message can be ignored.	
3.	Active SOAM CLI: View DA- MP status	 Enter the command: \$ upgradeHealthCheck daMpStatus This command outputs status to the screen for review. Note: The FIPS integrity verification test failed message may display when the upgradeHealthCheck command runs. This message can be ignored. Verify all peer MPs are available. Note the number of Total Connections Established	
4.	Compare data to the pre- upgrade health check to verify if the system has degraded after the second maintenance window	3. Note the number of Total Connections Established Verify the health check status of the upgraded site as collected in this procedure is the same as the pre-upgrade health checks taken in section 5.1.2. If system operation is degraded, it is recommended to report it to My Oracle Support (MOS).	

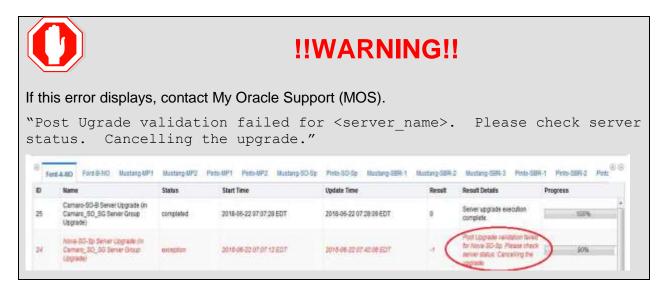
Note: If another site is to be upgraded, all procedures specified by Table 12 must be executed. However, the user should be aware that mated sites should not be upgraded in the same maintenance window.

5.4.3 Post-Upgrade Procedures

The procedures in this section are to be executed after the site upgrade is verified to be valid and healthy. These procedures should be executed in the maintenance window.

Procedure 30. Post-Upgrade Procedures

Step #	Procedure	Description			
Check of number	This procedure performs additional actions that are required after the upgrade is successfully completed. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	Active SOAM VIP: Enable the signaling firewall for the upgraded site	 The firewall enables the DSR to dynamically determine and customize the Linux firewall on each DA-MP server in the DSR Signaling node to allow only the essential network traffic pertaining to the active signaling configuration. There are some limitations related to enabling of signaling firewall in DSR 8.2 and later releases. See section 1.7.3 for more details. Navigate to Diameter > Maintenance > Signaling Firewall. Select the Signaling Node that was just upgraded. Click Enable. Click OK to confirm the action. Verify the Admin State changes to Enabled. Note: There may be a short delay while the firewall is enabled on the site. 			



6. Backout Procedure Overview

The procedures provided in this section return the individual servers and the overall DSR system to the source release after an upgrade is aborted. The backout procedures support two options for restoring the source release:

- Emergency backout
- Normal backout

The emergency backout overview is provided in Table 22. These procedures back out the target release software in the fastest possible manner, without regard to traffic impact.

The normal backout overview is provided in Table 23. These procedures back out the target release software in a more controlled manner, sustaining traffic to the extent possible.

All backout procedures are executed inside a maintenance window.

The backout procedure times provided in Table 22 and Table 23 are only estimates as the reason to execute a backout has a direct impact on any additional backout preparation that must be done.

Note: While not specifically covered by this procedure, it may be necessary to re-apply patches to the source release after the backout. If patches are applicable to the source release, verify all patches are on-hand before completing the backout procedures.

	Elapsed Ti	me (hr:min)		
Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 31	0:10-0:30	0:10-0:30	Procedure 31 The reason to execute a backout has a direct impact on any additional backout preparation that must be done. Since all possible reasons cannot be predicted ahead of time, only estimates are given here. Execution time varies.	None.
Procedure 32	0:01	0:11-0:31	Procedure 32	Disables global provisioning
Procedure 33	See Note	See Note	 Procedure 33 <i>Note</i>: Execution time of downgrading entire network is approximately equivalent to execution time taken during upgrade. 0:05 (5 minutes) can be subtracted from total time because ISO Administration is not executed during Backout procedures. 	All impacts as applicable in upgrade apply in this procedure. Also, backout procedures cause traffic loss.
Procedure 38	See Note	See Note	Procedure 38 Note : Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also, backout procedures cause traffic loss.

Table 22. Emergency Backout Procedure Overview

	Elapsed Time (hr:min)			
Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 34	See Note	See Note	Procedure 34 Note: Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also, backout procedures cause traffic loss.
Procedure 39	0:01-0:05	Varies	Procedure 39	None

Table 23. Normal Backout Procedure Overview

	Elapsed Tir	ne (hr:min)		
Procedure	This Step	Cum	Procedure Title	Impact
Procedure 31	0:10-0:30	0:10-0:30	Procedure 31	None
			The reason to execute a backout has a direct impact on any additional backout preparation that must be done. Since all possible reasons cannot be predicted ahead of time, only estimates are given here. Execution time varies.	
Procedure 32	0:01	0:11-0:31	Procedure 32	Disables global provisioning
Procedure 35	See Note	See Note	 Procedure 35 <i>Note</i>: Execution time of downgrading entire network is approximately equivalent to execution time taken during upgrade. 0:05 (5 minutes) can be subtracted from total time because ISO Administration is not executed during Backout procedures. 	All impacts as applicable in upgrade apply in this procedure. Also, backout procedures cause traffic loss.
Procedure 38	See Note	See Note	Procedure 38 Note : Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also, backout procedures cause traffic loss.
Procedure 36	See Note	See Note	Procedure 36 Note : Execution time of downgrading a single server is approximately equivalent to execution time to upgrade the server.	All impacts as applicable in upgrade apply in this procedure. Also, backout procedures cause traffic loss.
Procedure 39	0:01-0:05	Varies	Procedure 39	None

6.1 **Recovery Procedures**

It is recommended to direct upgrade procedure recovery issues to My Oracle Support (MOS). Before executing any of these procedures, it is recommended to contact My Oracle Support (MOS).

Execute this section only if there is a problem and it is desired to revert back to the pre-upgrade version of the software.



Before attempting to perform these backout procedures, it is recommended to first contact My Oracle Support (MOS) as described in Appendix Z.

Backout procedures cause traffic loss.

Note: These recovery procedures are provided for the backout of an Upgrade ONLY (i.e., from a failed 8.2 release to the previously installed 7.1.w release). Backout of an initial installation is not supported.

During the backout, servers may have the following expected alarms until the server is completely backed out. The servers may have some or all of the following expected alarms, but are not limited to event IDs:

- Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)
- Alarm ID = 31109 (Topology config error)
- Alarm ID = 31114 (DB Replication over SOAP has failed)
- Alarm ID = 31106 (DB Merge To Parent Failure)
- Alarm ID = 31134 (DB replication to slave failure)
- Alarm ID = 31102 (DB replication from master failure)
- Alarm ID = 31282 (HA management fault)

6.2 Backout Health Check

This section provides the procedure to verify that the DSR is ready for backout. The site post-upgrade Health Check is used to perform the backout Health Check.

Procedure 31. Backout Health Check

Step #	Procedure	Description			
This pro	This procedure performs a Health Check on the site prior to backing out the upgrade.				
Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.					
If this pr	If this pressdure fails, it is recommended to contact My Oracle Support (MOS) and call for assistance				

If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

Step #	Procedure	Description						
1.	Active NOAM	1. Navigate to Administration > Software Management > Upgrade.						
	VIP: Run the	 Select the SOAM tab of the site being backed out. 						
	automated post-upgrade		SOAM serve		•		a backed out	
	health checks for backout		active SOAM	• ·			g buonoù oun	
		Main Menu: Adm	inistration -> Sof	tware Mana	gement -> Upg	rade		
		Filter* • Tasks •	1:					
		BanA_BINDING_SG	BanA_MP_SG BanA_	SO_SG STXA	MP_SG GTXA_NO	SG GTXA	SESSION_SG GTXA	\$0_\$0
		Hostname		OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO	
		07XA-S01	Accept or Reject	******************	System CAM	CAM	9.0.0.0.0-60.13.0	
		L	Accept or Reject	Standby	GTXA_1111101_90 System OAM	OAM	0.0.0.0.00.0.00.13.0	H#86_64.180
		GTXA-SO-SP		NIA	GTXA_1111101_80		DSR-60.000_80.130	-x86_64.isc
		5. Click Che 6. Under Hea	checkup beckup A ckup. alth check opt	A CANTONNA			1AII	
		 Click Chee Under Hea Click OK. 	ckup. alth check opt	tions, clic	k Post Upg		t All	
		 Click Chee Under Hea Click OK. Control ret 	ckup. alth check opt turns to the U	tions, clic	k Post Upg creen.	rade.		
		 Click Chee Under Hea Click OK. Control ret 	ckup. alth check opt	tions, clic	k Post Upg creen.	rade.		neckup]
		 Click Chee Under Hea Click OK. Control ret Main Menu: A 	ckup. alth check opt turns to the U	tions, clic	k Post Upg creen. are Manager	rade.		neckup]
		 Click Chee Under Hea Click OK. Control ret 	ckup. alth check opt turns to the U	tions, clic	k Post Upg creen.	rade.		neckup]
		 5. Click Chee 6. Under Hea 7. Click OK. Control ret Main Menu: A Hostname Act 	ckup. alth check opt turns to the U	tions, clic	k Post Upg creen. are Manager Status OAM HA. Role	rade. ment -:	> Upgrade [Cf	Applic
		 5. Click Chee 6. Under Hea 7. Click OK. Control ret Main Menu: A Hostname Act 	ckup. alth check opt turns to the U dministration	tions, clic	k Post Upg creen. are Manager	rade. ment -:	> Upgrade [Cł	
		 5. Click Chee 6. Under Hea 7. Click OK. Control ret Main Menu: A Hostname Act 	ckup. alth check opt turns to the U dministration	tions, clic	k Post Upg creen. are Manager Status OAM HA. Role	rade. ment -:	> Upgrade [Cf	Applic
		5. Click Chee 6. Under Hea 7. Click OK. Control ret Main Menu: A Hostname Act GTXA. SO1 He Health check options Checkup Type	ckup. alth check opt turns to the U dministration	tions, clic	k Post Upg creen. are Manager Status OAM HA. Role	rade. ment -:	> Upgrade [Cf	Applic
		5. Click Chee 6. Under Hea 7. Click OK. Control ref Main Menu: A Hostname Act GTXA.SO1 He Health check options Checkup Type	ckup. alth check opt turns to the U administration kon alth Check Advance Upgrade Pre Upgrade	tions, clic	k Post Upg creen. are Manager Status GAM HA Role Active	rade. ment -3 Neta 07X4	> Upgrade [Cf	Applic
		5. Click Chee 6. Under Hea 7. Click OK. Control ref Main Menu: A Hostname Act GTXA.SO1 He Health check options Checkup Type	ckup. alth check opt turns to the U administration kon edith Check Relupgrade Prelupgrade Presupgrade	tions, clic	k Post Upg creen. are Manager Status OAM HA Role Active	rade. ment -3 Neta 07X4	> Upgrade [Cf ork Element _1111101_90 Ormedia Sile.	Apple

Step #	Procedure	Description				
2.	Active NOAM VIP: Monitor health check	 Click the Tasks option to display the currently executing tasks. The Health Check task name appears as <soservergroup> PostUpgrade Health Check.</soservergroup> 				
	progress for completion	 Monitor the Health Check task until the Task State is completed. The Details column displays a hyperlink to the Health Check report. 				
		3. Click the hyperlink to download the Health Check report.				
		4. Open the report and review the results.				
		Main Menu: Administration -> Software Management -> Upgrade				
		Filler" - Status - Tasks" -				
		Bank_BNOND_SO ID Hostname Name Task State Details Progress				
		Hostname 45 GTXA-NO1 GTXA_SO_SG PostJograde_HoathCheck_G PostJograde Hoath Check				
		GTXA-SO1 45 GTXA-NO1 0TXA-Session2 Server completed completed completed completed complete complete				
		GTXA-SO-SP GTXA-Season1 Server				
3.						
	VIP: Analyze health check results	 Analyze health check report for failures. If the Health Check report status is anything other than Pass, the Health Check logs can be analyzed to determine if the upgrade can proceed. 1. Navigate to Status & Manage > Files. 2. Select the active SOAM tab. 3. Select the UpgradeHealthCheck.log file and click View. 4. Locate the log entries for the most recent health check. Review the log for failures. Analyze the failures and determine if it is safe to continue the upgrade. If necessary, it is recommended to contact My Oracle Support (MOS) for guidance. 				
4.	Active NOAM VIP: Identify	1. Navigate to Administration > Software Management > Upgrade.				
	IP addresses	2. Select the SOAM tab of the site being backed out.				
	of servers to be backed out	 Select each server group link, making note of the application version of each server. 				
		 Based on the Application Version column, identify all the hostnames that need to be backed out. 				
		5. Navigate to Configuration > Servers .				
		 Using the data recorded in Table 5, note the XMI/iLO/LOM IP addresses of all the hostnames to be backed out. These are required to access the server when performing the backout. 				
		The reason to execute a backout has a direct impact on any additional backout preparation that must be done. The backout procedures cause traffic loss. Since all possible reasons cannot be predicted ahead of time, it is recommended to contact My Oracle Support (MOS) as stated in the Warning box.				

Step #	Procedure	De	scription					
5.	Active NOAM	1.	Navigate to	Status & Manag	e > Files.			
	VIP: Verify backup archive files	2.						
			Backup. <a< th=""><th>application>.</th><th><server></server></th><th>.FullDBPart</th><th>s.<ro< th=""><th>le>.<date_< th=""></date_<></th></ro<></th></a<>	application>.	<server></server>	.FullDBPart	s. <ro< th=""><th>le>.<date_< th=""></date_<></th></ro<>	le>. <date_< th=""></date_<>
			Backup.	ion>. <server></server>	>.FullRu	nEnv. <role></role>	•. <date< th=""><th>e_time>.UP</th></date<>	e_time>.UP
6. □	Active NOAM CLI: Verify disk usage	 Starting with the active SOAM, log into each service the disk usage is within acceptable limits. Use the SSH command (on UNIX systems – windows) to log into the active SOAM. 						-
			ssh admus	sr@ <server ip:<="" th=""><th>></th><th></th><th></th><th></th></server>	>			
			password:	<pre><enter pass<="" pre=""></enter></pre>	word>			
			Answer yes	if you are asked	to confirm	the identity of	the serv	er.
		2.	Enter the co	ommand:				
			[admusr@E	CVO-NO-1 ~]\$ d	df			
			Sample out	put (abridged):				
		Fi on	lesystem	1K-blocks	Used	Available	Use%	Mounted
		/d	ev/mapper/	'vgroot-plat_	root			
				999320	294772	652120	32%	/
			pfs	12303460	0			/dev/shm
			ev/vda1	245679		190605	19%	/boot
		/d	ev/mapper/	'vgroot-plat_1		045044	1.0	
		(a		999320		945344	18	/tmp
		70	ev/mapper/	vgroot-plat_u		1804824	<mark>63%</mark>	lisr
		/d	ev/mapper/	vgroot-plat v		1004024	000	
		/ 04	ov, mappor,	999320	558260	388632	<mark>59%</mark>	/var
		/d	ev/mapper/	'vgroot-plat v	var tklc			
				—		870380	78%	/var/TKLC
		3.	<mark>70</mark> % or less	e line for the /var a , this procedure is mergency) or Tab	s complete	. Continue wit		
		4.	partition for selecting fi could seve	of the /var and /u files that can be s les to be deleted rely impair the D step for all serve	safely dele I. The del ISR functi	ted. Use extre etion of critica onality.	eme cau	ution in

6.3 Disable Global Provisioning

The following procedure disables provisioning on the NOAM. This step ensures no changes are made to the database while the NOAMs and sites are backed out. Provisioning is re-enabled once the NOAM upgrade is complete.

Procedure 32	Disable Global	Provisioning
--------------	----------------	--------------

Step #	Procedure	De	scription
Otep #	Troccure		
This pro	cedure disables p	rovis	ioning for the NOAM servers, prior to upgrade.
Check o number.		s it is	completed. Boxes have been provided for this purpose under each step
If this pr	ocedure fails, it is	reco	mmended to contact My Oracle Support (MOS) and ask for assistance.
1.	Active NOAM VIP: Disable	1.	Log into the active NOAM GUI using the VIP.
	global	2.	Navigate to Status & Manage > Database.
	provisioning and	3.	Click Disable Provisioning.
	configuration	4.	Confirm the operation by clicking OK on the screen.
	updates on the entire network	5.	Verify the button text changes to Enable Provisioning . A yellow information box should also be displayed at the top of the view screen which states:
			[Warning Code 002] – Global provisioning has been manually disabled.
			The active NOAM server has the following expected alarm:
			Alarm ID = 10008 (Provisioning Manually Disabled)

6.4 Perform Emergency Backout

EMERGENCY SITE BACKOUT

Use this section to perform an emergency backout of a DSR upgrade.

The procedures in this section perform a backout of all servers to restore the source release. An emergency backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. It is recommended to contact My Oracle Support (MOS) as stated in the warning box in Section 6.1, to verify that all corrective setup steps have been taken.

6.4.1 Emergency Site Backout

The procedures in this section backout all servers at a specific site without regard to traffic impact.



Step #	Procedure	Description
		the DSR application software from multiple B- and C-level servers for a equiring backout can be included: SOAMs, DA-MPs, IPFEs, and SBRs.
Check o number.		it is completed. Boxes have been provided for this purpose under each step
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.
1.		1. Log into the NOAM GUI using the VIP.
	VIP: Identify all servers that	2. Navigate to Administration >Software Management >Upgrade.
	require backout (within a site)	3. Select the SOAM tab of the site being backed out.
	(within a site)	4. Select each server group link, making note of the application version of the servers.
		 Identify the servers in the respective server groups with the target release Application Version value. These servers were previously upgraded but now require backout.
		6. Make note of these servers. They have been identified for backout.
		 Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.
2.	Active SOAM	1. Log into the SOAM GUI using the VIP.
	VIP: Disable site	2. Navigate to Status & Manage > Database.
	provisioning for	3. Click Disable Provisioning.
	the site to be backed out	4. Confirm the operation by clicking OK on the screen.
		Verify the button text changes to Enable Provisioning. A yellow information box displays at the top of the view screen which states:
		[Warning Code 004] – Site provisioning has been manually disabled.
		The active SOAM server has the following expected alarm:
		Alarm ID = 10008 (Provisioning Manually Disabled)
C	!!WAF	RNING!! Step 3 results in a total loss of all traffic being processed by this DSR.
3.	Back out all C-	For all configurations:
	level servers, as applicable	Back out all C-level servers (IPFEs, SBRs, SBRs, and DA-MPs) identified in step 1:
		Execute Procedure 38.
4. □	Additional post back out steps	After all the servers in a particular server group are backed out, revert back the changes for the SBR server by executing Appendix L Additional Post-Backout Steps.
		Perform Appendix U to create a link of Comagent.

Procedure 33. Emergency Site Backout

Step #	Procedure	Description	
5.	Back out the standby and spare SOAM servers, as applicable	 Back out the standby and spare DSR SOAM servers: If standby and spare SOAM servers are present: Execute Procedure 38. If only a spare SOAM server is present: Execute Procedure 37. 	
6. □	Back out the active DSR SOAM server	Execute Procedure 37.	
7.	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the SOAM server(s) by executing Appendix L Additional Post-Backout Steps.	
8.	Active SOAM VIP: Enable site provisioning	 Log into the SOAM GUI using the VIP. Navigate to Status & Manage > Database. Click Enable Site Provisioning. Confirm the operation by clicking OK on the screen. Verify the button text changes to Disable Site Provisioning. 	

Note: If another site is to be backed out, follow all procedures in Table 22 in another maintenance window.

6.4.2 Emergency NOAM Backout

The procedures in this section backout the NOAM servers.

Procedure 34. Emergency NOAM Backout

Step #	Procedure	Description					
NOAM s	This procedure is used to perform an emergency backout of the DSR application software from the NOAM servers. This procedure backs out the application software as quickly as possible, without regard to operational impact.						
number.		it is completed. Boxes have been provided for this purpose under each step recommended to contact My Oracle Support (MOS) and ask for assistance.					
1.	Back out the standby DR NOAM server (if equipped)	Execute Procedure 37.					

Step #	Procedure	Description
2.	Back out the active DR NOAM server (now the standby) (if equipped)	Execute Procedure 37.
3.	Back out the standby DSR NOAM server (as applicable)	Execute Procedure 37.
4.	Back out the active DSR NOAM server (now the standby)	Execute Procedure 37.
5.	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the NOAM server(s) by executing Appendix L Additional Post-Backout Steps.
6.	Active NOAM VIP: Enable global provisioning and configuration updates on the entire network	 Log into the NOAM GUI using the VIP. Navigate to Status & Manage > Database. Click Enable Provisioning. Verify the button text changes to Disable Provisioning.

Step #	Procedure	Description	
7.	Active NOAM	1. Navigate to Status & Manage > Servers.	
	VIP: Remove Ready state for any backed out server	2. If any backed-out server Application Status is Disabled , then navigate to the server row and click Restart .	
		3. Navigate to Administration >Software Management >Upgrade.	
		 If any backed-out server shows an Upgrade State of Ready or Success, then select that server and click Complete Upgrade. Otherwise, skip this step. 	
		5. Click OK .	
		This removes the Forced Standby designation for the backed-out server.	
		No	<i>Note</i> : Due to backout being initiated from the command line instead of through the GUI, the following SOAP error may appear in the GUI banner.
		SOAP error while clearing upgrade status of hostname=[frame10311b6] ip=[172.16.1.28]	
		It is safe to ignore this error message.	
		6. Verify the Application Version value for servers has been downgraded to the original release version.	

6.5 Perform Normal Backout



The following procedures to perform a normal backout can only be executed once all necessary corrective setup steps have been taken to prepare for the backout. It is recommended to contact My Oracle Support (MOS), as stated in the warning box in Section 6.1, to verify that all corrective setup steps have been taken.

6.5.1 Normal Site Backout

The procedures in this section backs out all servers at a specific site.

Step #	Procedure	Description
		an upgrade of the DSR application software from multiple servers in the ring backout can be included: SOAMs, DA-MPs, IPFEs, and SBRs.
Check o number.	· / ·	it is completed. Boxes have been provided for this purpose under each step
		recommended to contact My Oracle Support (MOS) and ask for assistance.

Procedure 35. Normal Site Backout

Step #	Procedure	Description
1.	Active NOAM	1. Log into the NOAM GUI using the VIP.
	VIP: Identify all servers that	2. Navigate to Administration >Software Management > Upgrade.
	require backout	3. Select the SOAM tab of the site being backed out.
	(within a site)	4. Select each server group link, making note of the application version of each server.
		 Identify the servers in the respective Server Groups with the target release Application Version value. These servers were previously upgraded but now require Backout.
		6. Make note of these servers. They have been identified for backout.
		 Before initiating the backout procedure, remove all new blades and/or sites configured after upgrade was started.
2.	Active SOAM	1. Log into the SOAM GUI using the VIP.
	VIP: Disable site	2. Navigate to Status & Manage > Database.
	provisioning for	3. Click Disable Provisioning.
	the site to be backed out	4. Confirm the operation by clicking OK on the screen.
		5. Verify the button text changes to Enable Provisioning . A yellow information box displays at the top of the view screen which states:
		[Warning Code 004] – Site provisioning has been manually disabled.
		The active SOAM server has the following expected alarm:
		Alarm ID = 10008 (Provisioning Manually Disabled)
3.	Back out the first set of C- level servers,	<i>Note</i> : In a PCA System, the spare SBR server is located at the mated site of the site being backed out.
	as applicable	These servers can be backed out in parallel (as applicable):
		 ½ of all DA-MPs for N+0 (multi-active) configuration
		Standby SBR(s)
		Spare SBR(s)
		• ½ of all IPFEs
		Execute Procedure 37 for each standby/spare C-level server identified.

Step #	Procedure	Description			
4.	Active NOAM VIP: Verify standby SBR server status	If the server being backed out is the standby SBR, execute this step Otherwise, continue with step 6. Navigate to SBR > Maintenance > SBR Status. Open the tab server group being upgraded. Do not proceed to step 6 until the Resource HA Role for the st server has a status of Standby. BINDING SESSION Server Group Name Resource Domain Name BINIDING_SG			e tab of the
		GTXA_SESSION_SG		SESSION	
		Server Name	Resource HA Ro	le Conge	estion Level
		BarrA-Session-SP	Spare	Norma	al
		GTXA-Session1	Active	Norma	al
		GTXA-Session2	Standby	Norma	al
	VIP: Verify bulk download is complete between the active SBR in the server group to the standby and spare SBRs	 Navigate to Alarm & Event > View History. Export the Event log using the following filter: Server Group: Choose the SBR group that is in upgrade Display Filter: Event ID = 31127 – DB Replication Audit Complete Collection Interval: X hours ending in current time, where X is the time from upgrade completion of the standby and spare servers to the current time. Wait for the following instances of Event 31127: 1 for the Standby Binding SBR server 1 for the Standby Session SBR server 1 for the Spare Binding SBR server 1 for the Spare Binding SBR server 1 for the 2nd Spare Binding SBR server, if equipped 1 for the 2nd Spare Session SBR server, if equipped 1 for the is an expected loss of traffic depending on size of the bulk download. This must be noted along with events captured. 			
6.	Back out remaining C- level servers, as applicable	 These servers can be backed out in parallel (as applicable) ½ of all DA-MPs for N+0 (multi-active) configuration Active SBR(s) ½ of all IPFEs Execute Procedure 37 for each C-level server identified. 			

Step #	Procedure	Description	
7.	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the SBR server(s) by executing Appendix L Additional Post- Backout Steps.	
8.	Back out the standby DSR SOAM server	Execute Procedure 37.	
9.	Back out spare DSR SOAM server, if applicable	Note: The spare server is located at the mated site of the site being backed out. Execute Procedure 37.	
10. □	Back out active DSR SOAM server	Execute Procedure 37.	
11.	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the SOAM server(s) by executing Appendix L Additional Post-Backout Steps. Perform Appendix U to create a link of Comagent.	
12.	Active SOAM VIP: Enable site provisioning	 Log into the SOAM GUI using the VIP. Navigate to Status & Manage > Database. Click Enable Site Provisioning. Confirm the operation by clicking OK on the screen. Verify the button text changes to Disable Site Provisioning. 	

Note: If another site is to be backed out, follow all procedures in Table 23 in another maintenance window.

6.5.2 Normal NOAM Backout

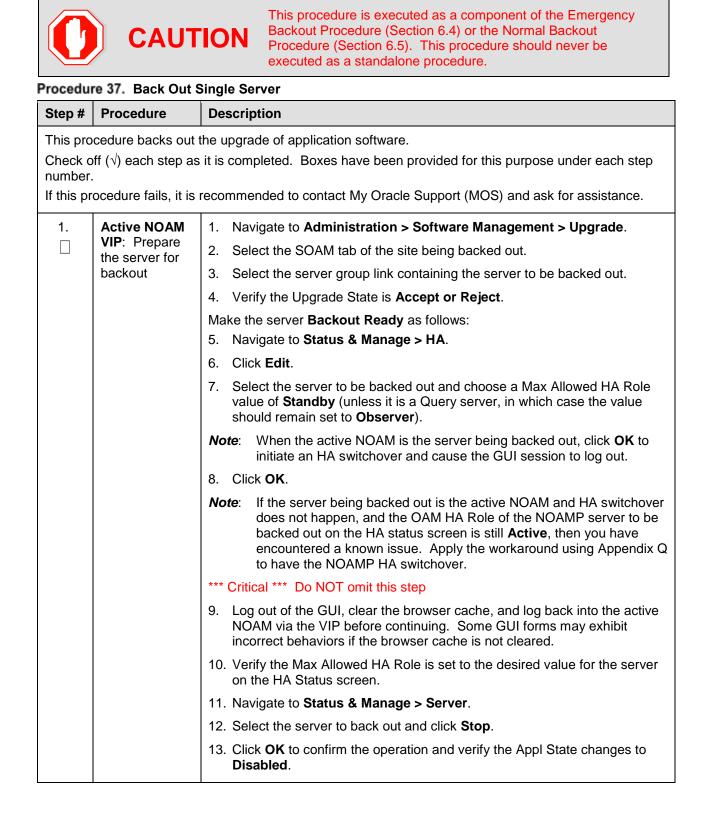
The procedures in this section backout the NOAM servers.

Procedure 36. Normal NOAM Backout

Step #	Procedure	Description		
-	This procedure is used to perform a normal backout of the DSR application software from the NOAM servers.			
Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.		
1.	Back out the standby DR NOAM server (if equipped)	Execute Procedure 37.		
2.	Back out other DR NOAM server (if equipped)	Execute Procedure 37.		
3.	Back out standby DSR NOAM server (as applicable)	Execute Procedure 37.		
4.	Back out active DSR NOAM server	Execute Procedure 37.		
5.	Additional post backout steps	After all the servers in a particular server group are backed out, revert back the changes for the NOAM server(s) by executing Appendix L Additional Post-Backout Steps.		
6.	Active NOAM VIP: Enable global provisioning and configuration updates on the entire network	 Log into the NOAM GUI using the VIP. Navigate to Status & Manage > Database. Click Enable Provisioning. Verify the button text changes to Disable Provisioning. 		

6.6 Back Out Single Server

This section provides the procedures to back out the application software on a single server.



Step #	Procedure	Description		
		14. Navigate to Administration > Software Management > Upgrade.		
		15. Select the SOAM tab of the site being backed out.		
		 Select the link of the server group containing the server to be backed out. Verify the Upgrade State is now Backout Ready. 		
		<i>Note</i> : It may take a couple of minutes for the status to update.		
2.	SSH to server ssh admusr@ <server address=""> password: <enter password=""> Note: If direct access to the IMI is not available, or if TVOE is insta</enter></server>			
		blade, then access the target server via a connection through the active NOAM. SSH to the active NOAM XMI first. From there, SSH to the target server's IMI address.		
3.	Server CLI: Execute the backout	Execute this command to find the state of the server to be backed out: \$ ha.mystate In this example, the HA state is Stb (highlighted). [admusr@MauiNOAM1 -]\$ ha.mystate		
		resourceId role node DC subResources lastUpdate		
		DbReplication Act/Stb A2260.016 0 0727:005354.362 VIP Act/Stb A2260.016 0 0727:005354.364 CacdProcessRes Act/Stb A2260.016 0 0727:005803.864 CAPM_HELP_Proc Act/OOS A2260.016 0 0727:005803.864 DSROAM_Proc Act/Stb A2260.016 0 0727:005803.996 CAPM_PSFS_Proc Act/Stb A2260.016 0 0727:005422.602 \$ sudo /var/TKLC/backout/reject \$ \$ \$ \$		
		<i>Note</i> : If back out asks to continue, answer y . The reject command creates a no-hang-up shell session, so the command continues to execute if the user session is lost.		
		Sample output of the reject script:		
		Applications Enabled. Running /usr/TKLC/plat/bin/service_conf reconfig Remove isometadata (appRev) file from upgrade Reverting platform revision file RCS_VERSION=1.4 Creating boot script: /etc/rc3.d/S89backout Rebuilding RPM database. This may take a moment rpmdb_load: /var/lib/rpm/Packages: unexpected file type or format Cleaning up chroot environment A reboot of the server is required. The server will be rebooted in 10 seconds		
- - .	proceeds	Many informational messages display to the terminal screen as the backout proceeds. After backout is complete, the server automatically reboots.		
5.	Server CLI: SSH to server	Use an SSH client to connect to the server (e.g., ssh, putty): ssh admusr@ <server address=""> password: <enter password=""></enter></server>		

Step #	Procedure	Description	
		Perform Appendix U to create a link of Comagent.	
6.	Server CLI: Restore the full DB run environment	Execute the backout_restore utility to restore the full database run environment: \$ sudo /var/tmp/backout_restore If asked to proceed, answer y.	
		Note : In some incremental upgrade scenarios, the backout_restore file is not found in the /var/tmp directory, resulting in the following error message:	
		<pre>/var/tmp/backout_restore: No such file or directory If this message occurs, copy the file from /usr/TKLC/appworks/sbin to /var/tmp and repeat sub-step 1.</pre>	
		The backout_restore command creates a no-hang-up shell session, so the command continues to execute if the user session is lost.	
		If the restore was successful, the following displays: Success: Full restore of COMCOL run env has completed.	
		Return to the backout procedure document for further instruction.	
		If an error is encountered and reported by the utility, it is recommended to consult with My Oracle Support (MOS) for further instructions.	
7.	Server CLI: Verify the backout	 Examine the output of the following commands to determine if any errors were reported: 	
		\$ sudo verifyUpgrade	
		Note: The verifyUpgrade command detected errors that occurred in the initial upgrade and during the backout. Disregard the initial upgrade errors.	
		<i>Note</i> : Disregard the TKLCplat.sh error:	
		[root@NO1 ~]# verifyUpgrade	
		ERROR: TKLCplat.sh is required by upgrade.sh!	
		ERROR: Could not load shell library!	
		ERROR: LIB:	
		/var/TKLC/log/upgrade/verifyUpgrade/upgrade.sh ERROR: RC: 1	
		Also, disregard this error: ERROR: Upgrade log	
		<pre>(/var/TKLC/log/upgrade/upgrade.log) reports errors! ERROR: 1513202476::zip error: Nothing to do!</pre>	
		/usr/share/tomcat6/webapps/ohw.war	
		This command displays the current sw rev on the server:	
		\$ appRev	
		Install Time: Wed Apr 4 05:03:13 2018	
		Product Name: DSR	
		Product Release: 8.6.0.0.0_95.14.0	

Step #	Procedure	Description
		Base Distro Product: TPD
		Base Distro Release: 7.7.0.0.0-88.68.0
		Base Distro ISO: TPD.install-7.7.0.0.0_88.68.0-
		OracleLinux6.10-x86_64.iso
		ISO name: DSR-DSR-8.6.0.0.0_95.14.0- x86_64.iso
		OS: OracleLinux 6.10
		2. Enter this command
		\$ sudo verifyBackout
		The verifyBackout command searches the upgrade log and report all errors found.
		 If the backout was successful (no errors or failures reported), then proceed to step 8.
		4. If the backout failed with the following error, this error can be ignored and the backout may continue.
		ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!
		ERROR: 1485165801::ERROR: <rpm name="">-7.2.14- 7.2.0.0.0_72.23.0: Failure running</rpm>
		command '/usr/TKLC/appworks/bin/eclipseHelp reconfig'
		Also, disregard following error.
		ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!
		ERROR: 1513202476::zip error: Nothing to do!
		/usr/share/tomcat6/webapps/ohw.war
		5. If the backout failed with the following error, refer to Appendix Y for the workaround:
		Running /usr/TKLC/plat/bin/service conf reconfig
		ERROR: Partially installed package was found:
		ERROR: TKLCdsr.x86_64
		ERROR: Partial packages exist!
		ERROR: Partial packages must be fixed before re-trying an upgrade!
		Remove isometadata (appRev) file from upgrade
		Restore original initrd images
		Reverting platform revision file
		RCS_VERSION=1.12
		ERROR: Backing out changes from BACKOUT_SERVER on backwards
		ERROR: Backout was unsuccessful!!!
		ERROR: Trouble when running backout command!

Step #	Procedure	Description			
		ERROR: CMD: /var/TKLC/backout/ugwrapbackout			
		ERROR: Failed to reject upgrade.			
		Rebuilding RPM database. This may take a moment			
		<pre>rpmdb_load: /var/lib/rpm/Packages: unexpected file type or format</pre>			
		Cleaning up chroot environment			
		Stopping remoteExec background process			
		Shutting down /var/TKLC/backout/remoteExec			
		/usr/TKLC/plat/sbin/savelogs_plat logs:			
		1530516317::ERROR: TKLCdpi-8.0.33-8.0.1.0.0_80.28.0: Adding the DSR helpset			
		failed!			
		1530516320::error: %post(TKLCdpi-0:8.0.33- 8.0.1.0.0_80.28.0.x86_64) scriptlet			
		failed, exit status 1			
		6. If the backout failed with the following error:			
		ERROR: The upgrade log does not exist!			
		Examine the upgrade log at /var/TKLC/log/upgrade/upgrade.log for errors that occurred during the backout.			
		If the backout failed due to errors found in the upgrade log, it is recommended to contact My Oracle Support (MOS) for further instructions.			
8.	Server CLI:	Enter this command to reboot the server:			
	Reboot the server	\$ sudo init 6			
	361761	This step can take several minutes.			
9.	Server CLI: Verify OAM services restart (NOAM/SOAM	If the server being backed out is a NOAM or SOAM, perform this step; otherwise proceed to step 10.			
		1. Wait several (approximately 6 minutes) minutes for a reboot to complete			
	o o b v)	before attempting to log back into the server.			
	only)	before attempting to log back into the server.2. SSH to the server and log in.			
	only)	2. SSH to the server and log in.			
	only)	2. SSH to the server and log in.			
	only)	2. SSH to the server and log in. login as: admusr			
	only)	<pre>2. SSH to the server and log in. login as: admusr password: <enter password=""></enter></pre>			
	only)	 SSH to the server and log in. <pre>login as: admusr password: <enter password=""> </enter></pre> Execute the following command to verify the httpd service is running. <pre>\$ sudo service httpd status</pre> The expected output displays httpd is running (the process IDs are			
	only)	 SSH to the server and log in. <pre>login as: admusr password: <enter password=""></enter></pre> Execute the following command to verify the httpd service is running. <pre>\$ sudo service httpd status</pre> 			
	only)	 SSH to the server and log in. <pre>login as: admusr password: <enter password=""> <pre>secure the following command to verify the httpd service is running. \$ sudo service httpd status The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored): httpd <process be="" here="" ids="" listed="" will=""> is running If httpd is not running, repeat sub-steps 3 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended to contact My Oracle Support (MOS) for further</process></pre></enter></pre> 			
	only)	 SSH to the server and log in. <pre>login as: admusr password: <enter password=""> <pre>secure the following command to verify the httpd service is running. \$ sudo service httpd status The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored): httpd <process be="" here="" ids="" listed="" will=""> is running If httpd is not running, repeat sub-steps 3 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended to contact My Oracle Support (MOS) for further instructions.</process></pre></enter></pre> 			
	only)	 SSH to the server and log in. <pre>login as: admusr password: <enter password=""> <pre>secure the following command to verify the httpd service is running. \$ sudo service httpd status The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored): httpd <process be="" here="" ids="" listed="" will=""> is running If httpd is not running, repeat sub-steps 3 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended to contact My Oracle Support (MOS) for further</process></pre></enter></pre> 			

Step #	Procedure	Description		
10.	Active NOAM VIP: Verify server state is correct after back out	 sudo ls -ltr /home/awadmin/.ssh/ The file permission should be defined as shown: [admusr@HPC-N01 ~]\$ sudo ls -lrt /home/awadmin/.ssh/total 20 -rw 1 awadmin awadm 1281 Sep 27 16:19 config -rw 1 awadmin awadm 605 Nov 18 13:20 1d_dsa.pub -rw 1 awadmin awadm 668 Nov 18 13:20 1d_dsa -rw 1 awadmin awadm 7275 Nov 18 18:09 authorized_keys 2. If the file ownership is not set for awadmin, then change the permission: sudo chown awadmin:awadm /home/awadmin/.ssh/id_dsa 3. Verify file ownership is changed to awadmin awadm. 1. Navigate to Administration > Software Management > Upgrade to observe the server upgrade status. 2. Select the SOAM tab of the site being backed out. 3. Select the link of the server group containing the server being backed out. If the server status is Not Ready, proceed to the next step; otherwise, 		
11.	Active NOAM VIP: Change/Correc t the Upgrade State on backed out server to Ready	 If the server status is Not Ready, proceed to the next step; otherwise, proceed to step 12. Navigate to Status & Manage > HA. Click Edit. Select the backed out server and choose a Max Allowed HA Role value of Active (unless it is a Query server, in which case the value should remain set to Observer). Click OK. Verify the Max Allowed HA Role is set to the desired value for the server on the HA Status screen. Navigate to Status & Manage > Server. Select the server being backed out and click Restart. Click OK to confirm the operation. Verify the Appl State updates to Enabled. Navigate to Administration > Software Management > Upgrade. Select the tab of the server group containing the server to be backed out. Verify the Upgrade State is now Ready. It may take a couple minutes for the grid to update. 		
12.	Active NOAM VIP: Verify application version is correct for the backed out server	 Navigate to Administration > Software Management > Upgrade. Select the SOAM tab of the site being backed out. Select the link of the server group containing the server that was backed out. Verify the Application Version value for this server has been downgraded to the original release version. 		

Step #	Procedure	Description
13.	Additional backout steps	To support backout for major upgrade paths on the NOAM, SOAM, and SBR server(s), execute Appendix K (Additional Backout Steps).

6.7 Back Out Multiple Servers

This section provides the procedures to backout the application software on multiple servers.

Procedure 38. Back Out Multiple Servers

Step # Procedure	Description
------------------	-------------

This procedure backs out the upgrade of DSR 8.6.0.0.0 application software for multiple servers. Any server requiring a backout can be included: DA-MPs, IPFEs, and SBRs.

Check off ($\sqrt{}$) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1.	Active NOAM VIP: Prepare the	1. Navigate to Administration > Software Management > Upgrade.
		2. Select the server group tab containing the server to be backed out.
	server for backout	3. Verify the Upgrade State is Accept or Reject.
	DACKOUL	Make the server Backout Ready as follows:
		4. Navigate to Status & Manage > HA.
		5. Click Edit.
		6. Select the server to back out and select a Max Allowed HA Role value of Standby (unless it is a Query server, in which case the value should remain set to Observer).
		Note: When the active NOAM is the server being upgraded, click OK to initiate an HA switchover and cause the GUI session to log out. Before logging into the active OAM again, close and re-open the browser using the VIP address for the NOAM, and clear the browser cache. Some GUI forms may exhibit incorrect behaviors if the browser cache is not cleared.
		7. Click OK .
		8. Verify the Max Allowed HA Role is set to the desired value for the server on the HA Status screen.
		9. Navigate to Status & Manage > Server.
		10. Select the server to back out and click Stop .
	•	

Step #	Procedure	Description			
	11. Click OK to confirm the operation and verify the Appl State chan Disabled .				
		12. Navigate to Administration > Software Management > Upgrade.			
		13. Select the SOAM tab of the site being backed out.			
		 Select the tab of the server group containing the server to be backed out. Verify the Upgrade State is now Backout Ready. 			
		<i>Note</i> : It may take a couple of minutes for the status to update.			
2.	Server CLI: Log into the server(s)	Use an SSH client to connect to the server (for example, ssh, putty): ssh admusr@ <server address=""> password: <enter password=""></enter></server>			
		Note: If direct access to the IMI is not available, then access the target server via a connection through the active NOAM. SSH to the active NOAM XMI first. From there, SSH to the target server's IMI address.			

Step #	Procedure	Description					
3.	Server CLI: Execute the	Determine the state either Standby or S		server to be	backed out. Th	e server role must be	
	backout	Execute following command to find the server role :					
		\$ ha.mystate					
		In this example output, the HA state is Standby .					
		[admusr@SO2 ~]\$ ha.mystate					
			_		subResources	lastUpdate	
		DbReplication	Stby	B2435.024	0	0127:113603.435	
		VIP	Stby	B2435.024	0	0127:113603.438	
		SbrBBaseRepl	OOS	B2435.024	0	0127:113601.918	
		SbrBindingRes	OOS	B2435.024	0	0127:113601.918	
		SbrSBaseRepl	OOS	B2435.024	0	0127:113601.918	
		SbrSessionRes				0127:113601.918	
		CacdProcessRes	OOS	B2435.024	0	0127:113601.918	
		DA_MP_Leader	OOS	B2435.024	0	0127:113601.917	
		DSR_SLDB	OOS	B2435.024	0-63	0127:113601.917	
		VIP_DA_MP	OOS	B2435.024	0-63	0127:113601.917	
		EXGSTACK_Process				0127:113601.917	
						0127:113601.917	
		CAPM_HELP_Proc				0127:113603.272	
		DSROAM_Proc	OOS	B2435.024	0	0128:081123.951	
		If the state of the se	rver is	Active, then	return to step 1		
		Execute the reject command to initiate the backout:					
		\$ sudo /var/TKLC/backout/reject					
		<i>Note</i> : If back out asks to continue, answer y .					
		The reject command	d creat	es a no-hang	J-up shell sessio	on, so the command	
					1 15 1051.		
		Sample output of th	-	t script:			
		Applications Enabled. Running /usr/TKLC/plat/bin/service_conf reconfig					
		Remove isometadata (appRev) file from upgrade					
		Reverting platform revision file					
		RCS_VERSION=1.4 Creating boot script: /etc/rc3.d/S89backout					
		Rebuilding RPM database. This may take a moment					
		rpmdb_load: /var/l Cleaning up chroot			nexpected file	type or format	
		A reboot of the se	rver i:	s required.			
		The server will be			conds		
4.	Server CLI: Backout	Many informational proceeds.	messa	ges display t	o the terminal s	creen as the backout	
_	proceeds	After backout is con	nplete,	the server a	utomatically reb	oots.	
5.	Repeat for each server	Repeat steps 1 thro	ugh 4 f	for each serv	er to be backed	out.	
	to be backed out						

Step #	Procedure	Description			
6. □	Server CLI: Log into the server	Use an SSH client to connect to the server (for example, ssh, putty): ssh admusr@ <server address=""> password: <enter password=""></enter></server>			
7.	Server CLI: Restore the full DB run environment	<pre>Execute the backout_restore utility to restore the full database run environment: \$ sudo /var/tmp/backout_restore If asked to proceed, answer y. Note: In some incremental upgrade scenarios, the backout_restore file is not found in the /var/tmp directory, resulting in the following error message: /var/tmp/backout_restore: No such file or directory If this message occurs, copy the file from /usr/TKLC/appworks/sbin to /var/tmp and repeat sub-step 1. The backout_restore command creates a no-hang-up shell session, so the command continues to execute if the user session is lost. If the restore was successful, the following displays: Success: Full restore of COMCOL run env has completed. Return to the backout procedure document for further instruction. If an error is encountered and reported by the utility, it is recommended to consult with My Oracle Support (MOS) by referring to Appendix U of this document for further instructions.</pre>			
8.	Server CLI: Verify the backout	 1. Examine the output of the following commands to determine if any errors were reported: \$ sudo verifyUpgrade Note: The verifyUpgrade command detected errors that occurred in the initial upgrade and during the backout. Disregard the initial upgrade errors. Note: Disregard the TKLCplat.sh error: [root@NO1 ~]# verifyUpgrade ERROR: TKLCplat.sh is required by upgrade.sh! ERROR: Could not load shell library! ERROR: LIB: /var/TKLC/log/upgrade/verifyUpgrade/upgrade.sh ERROR: RC: 1 Also, disregard following error. ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors! ERROR: 1513202476::zip error: Nothing to do! /usr/share/tomcat6/webapps/ohw.war This command displays the current sw rev on the server: \$ appRev Install Time: Wed Apr 4 05:03:13 2018 			

Step #	Procedure	Description			
		Product Release: 8.6.0.0.0_95.14.0			
		Base Distro Product: TPD			
		Base Distro Release: 7.7.0.0.0-88.68.0			
		Base Distro ISO: TPD.install-7.7.0.0.0_88.68.0- OracleLinux6.10-x86_64.iso			
		ISO name: DSR-8.6.0.0.0_95.14.0-x86_64.iso			
		OS: OracleLinux 6.10			
		2. Enter this command			
		\$ sudo verifyBackout			
		The verifyBackout command searches the upgrade log and report all errors found.			
		3. If the backout was successful (no errors or failures reported), then proceed to step 9.			
		4. If the backout failed with the following error, this error can be ignored and the backout may continue.			
		ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!			
		ERROR: 1485165801::ERROR: <rpm name="">-7.2.14- 7.2.0.0.0_72.23.0: Failure running</rpm>			
		command '/usr/TKLC/appworks/bin/eclipseHelp reconfig'			
		Also, Disregard following error too			
		ERROR: Upgrade log (/var/TKLC/log/upgrade/upgrade.log) reports errors!			
		ERROR: 1513202476::zip error: Nothing to do!			
		/usr/share/tomcat6/webapps/ohw.war			
		5. If the backout failed with the following error:			
		ERROR: The upgrade log does not exist!			
		Examine the upgrade log at /var/TKLC/log/upgrade/upgrade.log for errors that occurred during the backout.			
		 If the backout failed due to errors found in the upgrade log, it is recommended to contact My Oracle Support (MOS) for further instructions. 			
9.	Server CLI: Reboot the	Enter the following command to reboot the server:			
	server	<pre>\$ sudo init 6 This step can take several minutes.</pre>			

Step #	Procedure	Description
	Server CLI: Verify OAM services restart (NOAM/SO AM only)	<pre>Idescription If the server being backed out is a NOAM or SOAM, perform this step; otherwise proceed to step 11. Perform Appendix U to create a link of Comagent. I. Wait several (approximately 6 minutes) minutes for a reboot to complete before attempting to log back into the server. SSH to the server and log in. login as: admusr password: <enter password=""> Execute the following command to verify the httpd service is running. \$ sudo service httpd status The expected output displays httpd is running (the process IDs are variable so the list of numbers can be ignored): httpd <process be="" here="" ids="" listed="" will=""> is running If httpd is not running, repeat sub-steps 3 and 4 for a few minutes. If httpd is still not running after 3 minutes, then services have failed to restart. It is recommended to contact My Oracle Support (MOS) for further instructions. Verify if the file id_dsa has required ownership: Check the ownership of the file: ls -ltr /home/awadmin/.ssh/ The file permission should be defined as shown: [admusr@HPC-NOI ~]\$ sudo ls -lrt /home/awadmin/.ssh/ -rw 1 awadmin awadm 1201 Sep 27 16:19 config -rw 1 awadmin awadm 1205 Sep 27 16:19 config -rw 1 awadmin awadm 7275 Nov 18 18:09 authorized_keys I for the file ownership is not set for awadmin, then change the permission: sudo chown awadmin:awadm /home/awadmin/.ssh/id_dsa Verify file ownership is changed to awadmin awadm.</process></enter></pre>
11.	Additional backout steps	To support backout for major upgrade paths, execute Appendix K (Additional Backout Steps).
12.	Repeat for each server backed out	Repeat steps 6 through 11 for each server backed out.
13.	Active NOAM VIP: Verify server state is correct after back out	 Navigate to Administration > Software Management > Upgrade to observe the server upgrade status. If the active NOAM is on release 8.0 or later, and the server status is Not Ready, proceed to the next step; otherwise, proceed to step 17.

Step #	Procedure	Description				
14.	Active	1. Navigate to Statu	ıs & Manage > HA.			
	NOAM VIP: Change/Cor	2. Click Edit.				
	rect the Upgrade State on		d out server and choose a Max A is a Query server, in which case			
	backed out server to	4. Click OK .				
	Ready	5. Verify the Max All the HA Status scr	lowed HA Role is set to the desir reen.	ed value for the server on		
		6. Navigate to Statu	ıs & Manage > Server.			
		7. Select the server	being backed out and click Rest	art.		
		8. Click OK to confir	0			
			tate updates to Enabled .			
		, , , , , , , , , , , , , , , , , , , ,	mont > Ungrado			
		10. Navigate to Administration > Software Management > Upgrade.				
		11. Select the tab of the server group containing the server to be backed out.				
		12. Verify the Upgrad	le State is now Ready .			
		13. Proceed to step 1	 to complete the procedure. 			
15.	Active	1. Log into the NOA	M GUI using the VIP.			
	NOAM VIP: Remove	2. Navigate to Statu	ıs & Manage > Server.			
	Upgrade	5	backed-out show an Appl State	of Enabled then multi-		
	Ready		rows and click Stop .	or Enabled , then make		
	status	4. Click OK to confir	rm the operation.			
		Main Menu: Status & Ma				
		Filter •	anage Poerrei			
		Network Element	Server Hostname	Appl State		
		EVONOAMP1	EVO-NO-1	Enabled		
		EVONDAMP1	EVO-NO-2	Enabled		
		EVOSOAMNE EVOSOAMNE	EV0-80-8p EV0-80-1	Enabled		
		EVOSOAMNE	EV0-50-1	Enabled		
		Transformer at	Errout	000		

Step #	Procedure	Description						
16.	Active	Correct the upgrade status on the backed out server.						
	NOAM VIP: Correct	1. Navigate to Administration > Software Management > Upgrade.						
	upgrade status on the backed out server	then select	the backed show Upgra	out server a ade State of	and click Co Not Read	ompleto , then	e of Ready or Success e. If the servers just proceed to the next	
		Fitter • Tasks •						
		NO_SG UP_SG	90_9G					
			Upgrade State	OAM Max HA Role	Server Role	Function	Application Version	
		Hostname	Server Status	Max Allowed HA Role	Network Element		Upgrade ISO	
		ND1	Not Ready	Active	Network CAM&P NO_DSR_VM	OAMAP	6 0.0-60 12 0	
		102	Ready	Standby	Network OAM&P NO_DSR_VM	OHMSP	6.0.0-60.12.0	
		4. Click OK . to active, w	hich causes	the server'	s Upgrade		the backed-out server change to Not Ready	
		4. Click OK. to active, w Main Menu: Administratio	This updates hich causes	the server'	s Upgrade	State to		
		4. Click OK. to active, w Main Menu: Administratio	This update: hich causes n -> Software Mana nets the Actor Nates rets	gement -> Upgrade Thereby Name Tool (Marcon Control of	s Upgrade	State to	o change to Not Ready	
		4. Click OK. to active, w Main Menu: Administration Main Main Menu: Administration Main Main Main Main Main Main Main Main	This updates hich causes n -> Software Mana needs Actor Mana Hith Man Actor Mana Hith Man Actor Mana Mana Mana Mana Mana Mana Mana Mana	s the server's gement -> Upgrade United the (b) Canal may appear	s Upgrade	State to	change to Not Ready	
		4. Click OK. to active, w Main Menu: Administration Menu: Administration The following S SOAP error	This updates hich causes n -> Software Mana net not any Advertises NOT Mana OAP error r or while	gement -> Upgrade Thereby Name Tool (Marcon Control of	s Upgrade	State to banner: statu	change to Not Ready	
		4. Click OK. to active, w Main Menu: Administration Menu: Administration The following S SOAP error	This updates hich causes n -> Software Mana Mana History Actor Nates OAP error r or while = [frame10	s the server's gement -> Upgrade Theory Num (% Canad may appear clearing 311b6] ip	s Upgrade	State to banner: statu	change to Not Ready	
17.	Active	 4. Click OK. to active, w Main Menu: Administration Main Menu: Administratin Menu Main Menu Main Menu: Admini	This updates hich causes n -> Software Mana and the Actor Mana OAP error r or while = [frame10 ore this error	the server's gement -> Upgrade Use Server (a) Server may appear clearing 311b6] ip r message.	s Upgrade	banner: statu 5.1.28	change to Not Ready	
17.	NOAM VIP:	 4. Click OK. to active, w Main Menu: Administration Main Menu: Administratin Menu Main Menu Main Menu: Admini	This updates hich causes n -> Software Mana Mine OAP error r or while = [frame10 ore this error Administra	s the server's gement -> Upgrade The ty Nation (Not Careful anay appear clearing 311b6] ip r message. ation > Soft	s Upgrade	banner: statu 5.1.28	change to Not Ready	
		 4. Click OK. to active, w Main Menu: Administration The following S SOAP error hostname It is safe to igno 1. Navigate to 2. Select the S 	This updates hich causes -> Software Mana OAP error r or while = [frame10 ore this error Administra SOAM tab o	the server's gement -> Upgrade User Note (Note that the Mage appear clearing 311b6] ig r message. ation > Soft f the site be	s Upgrade [complete] in the GUI upgrade p=[172.16 tware Mana ing backed	banner: statu 5.1.28 agemen out.	change to Not Ready	

6.8 Post-Backout Health Check

This procedure is used to determine the health and status of the DSR network and servers following the backout of the entire system.

Procedure 39. Post-Backout Health Check

Step #	Procedure	Description			
This pro backout	This procedure performs a basic health check of the DSR to verify the health of the system following a backout.				
Check o number.		it is completed. Boxes have been provided for this purpose under each step			
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	Active NOAM	1. Log into the NOAM GUI using the VIP.			
	VIP: Verify server status is	2. Navigate to Status & Manage > Server.			
	normal	 Verify Server Status is Normal (Norm) for Alarm (Alm), Database (DB) and Processes (Proc). 			
		4. Do not proceed with the upgrade if any server status is not Norm .			
		Do not proceed with the upgrade if there are any Major or Critical alarms.			
		Refer to Appendix J for details.			
		Note: It is recommended to troubleshoot if any server status is not Norm. A backout should return the servers to their pre-upgrade status.			
2.	Active NOAM	1. Navigate to Alarms & Events > View Active.			
	VIP: Log all current alarms	2. Click Report to generate an Alarms report.			
	in the system	 Save the report and print the report. Keep these copies for future reference. 			

6.9 IDIH Backout

The procedures in this section back out the Oracle, Application, and Mediation servers to the previous release.

6.9.1 Oracle Server Backout

Backout of Oracle Server is not supported for release 7.1 or later.

The Oracle server is backed out using the disaster recovery procedure documented in [5].

6.9.2 Mediation and Application Server Backout

The Mediation and Application servers are backed out using the disaster recovery procedure documented in [5].

Appendix A. Post Upgrade Procedures

Execute the procedures in this section only **AFTER** the upgrade of **ALL** servers in the topology is completed.

Appendix A.1. Accept Upgrade

Detailed steps for accepting the upgrade are provided in the procedure. TPD requires that upgrades be accepted or rejected before any subsequent upgrades may be performed. **Alarm 32532 Server Upgrade Pending Accept/Reject** displays for each server until one of these two actions is performed.

An upgrade should be accepted only after it is determined to be successful as the Accept is final. This frees up file storage but prevents a backout from the previous upgrade.

Note: Once the upgrade is accepted for a server, that server is not allowed to backout to a previous release.

Note: This procedure must be performed in a Maintenance Window.



Upgrade acceptance may only be executed with authorization from the customer.

Be advised that once an upgrade has been accepted, it is not possible to back out to the previous release.

Procedure 40. Accept Upgrade

Step #	Procedure	Description			
-	This procedure accepts a successful upgrade. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	It is recommended that this procedure be performed two weeks after the upgrade	Verify the upgraded system has been stable for two weeks or more. <i>Note</i> : It is not possible to back out after this is procedure is executed.			
2.	Active NOAM VIP: Execute this step if accepting a NOAM server. Log all current alarms present at the NOAM.	 Log all alarms before accepting the NOAM upgrade. 1. Log into the NOAM GUI. 2. Navigate to Alarms & Events > View Active. 3. Click Report to generate an Alarms report. 4. Save the report and/or print the report. Keep these copies for future reference. All other upgraded servers have the following expected alarm: Alarm ID = 32532 (Server Upgrade Pending Accept/Reject) 			

Step #	Procedure	Description
3.	Active SOAM VIP: Execute this step if accepting a SOAM server. Log all current alarms present at the SOAM.	 Log all alarms before accepting the SOAM upgrade. 1. Log into the SOAM GUI. 2. Navigate to Alarms & Events > View Active. 3. Click Report to generate an Alarms report. 4. Save the report and/or print the report. Keep these copies for future reference. All other upgraded servers have the following expected alarm: Alarm ID = 32532 (Server Upgrade Pending Accept/Reject)
4.	Active NOAM VIP: Accept upgrade for multiple servers	 Log into the NOAM GUI using the VIP. Navigate to Administration >Software Management >Upgrade. Select the SOAM tab of the site being upgraded. Note: The Site Accept button accepts the upgrade for every upgraded server at the selected site. This is the most efficient way to accept an upgrade. A manual alternative to this is to select the link of each server group in the site and use the Accept button to accept the upgrade of only the servers in the selected server group. Click Site Accept. Main Menu: Administration > Software Management > Upgrade File: Tosts * Tostst * Tosts * T
		Server Group Functions Upgrade Method Server Upgrade States 50_Bited ODR (antiwelvedus part) CAV (Bite) Accept or Reject (2/2) 90_Bited ODR (antiwelvedus part) Rek (00% or skedely) Accept or Reject (2/2) 197_EE1_50 IP Freet End Server Accept or Reject (1/3) 197_EE1_50 IP Freet End Server Accept or Reject (1/3) 197_EE1_50 IP Freet End Server Accept or Reject (1/3) 197_EE1_50 IP Freet End Server Accept or Reject (1/3) 197_EE1_50 IP Freet End Server Accept or Reject (1/3) 197_EE2_56 IP Freet End Server Accept or Reject (1/3) 197_EE2_56 IP Freet End Server Accept or Reject (1/3) 197_EE2_56 IP Freet End Server Accept or Reject (1/3) 197_EE2_56 IP Freet End Server Accept or Reject (1/3) 197_EE1_50 IP Freet End Server Rejort All 197_EE1_50 IP Freet End Server Rejort All 197_EE1_50 IP Freet End Server Rejort All 100

Appendix A.2. Undeploy ISO

After the upgrade has been accepted, run this procedure to undeploy all deployed ISOs. When an ISO is undeployed, the ISO is deleted from all servers in the topology except for the active NOAM. On the active NOAM, the ISO remains in the File Management Area.

This procedure can be run at any time after the upgrade has been accepted.

Procedure 41.	Undeploy ISO
---------------	--------------

Step #	Procedure	Description
Check o number.	ff ($ ightarrow$) each step as	In ISO from the DSR servers. Is it is completed. Boxes have been provided for this purpose under each step recommended to contact My Oracle Support (MOS) and ask for assistance.
1.	Active NOAM VIP: View the files in the file management area	 Log into the NOAM GUI using the VIP. Navigate to Status & Manage > Files.
2.	Active NOAM VIP: Start ISO undeploy sequence	 Select an ISO stored in the isos directory of the File Management Area. The ISO filename has the format: isos/DSR-8.6.0.0.0_95.14.0-x86_64.iso Click Undeploy ISO. Click OK on the confirmation screen to start the undeploy sequence.
3.	Active NOAM VIP: Monitor the ISO undeploy progress	 Select the ISO being deployed in step 2. Click View ISO Deployment Report. If some servers show the ISO as Deployed, click Back on the Files View screen. Periodically repeat sub-steps 1 through 3 until all servers indicate Not Deployed. Main Menu: Status & Manage -> Files [View] Main Menu: Status & Manage -> Files [View] Peployment report for DSR-3.0.0.0.0_80.13.0-#56_61.1801 Deployed on 16/16 servers. GTXA-8011 Deployed GTXA-9021 Deployed
		GTKA-MF1: Deployed GTKA-ME2: Deployed GTKA-Session1: Deployed GTKA-Binding-SF: Deployed Print Save Back

Step #	Procedure	Description
4.	Active NOAM VIP: Repeat as necessary	If there are additional ISOs in the File Management Area that need to be undeployed, repeat steps 2. and 3. as necessary.

Appendix A.3. Post Upgrade Accept Procedures

The following procedure is executed after the upgrade has been accepted

Procedure 42. Post Upgrade Accept Procedure.

Step #	Procedure	Description			
	This procedure performs miscellaneous actions that are required to be executed after the upgrade is accepted.				
Check o number.	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	Active NOAM CLI: Reset COMCOL compatibility flag	 This step is required only if the source release is pre-8.x. 1. Use an SSH client to connect to the active NOAM: ssh <noam address="" ip="" xmi=""> login as: admusr password: <enter password=""></enter></noam> Note: The static XMI IP address for each server should be available in Table 5. 2. Enter this command to reset the COMCOL backward compatibility flag. Backward compatibility is no longer required when all of the servers in the topology have been upgraded to release 8.0 or later. \$ iset -fvalue=0 LongParam where "name='cm.cm6compat'" Sample output: 			
		<pre>=== changed 1 records === 3. Verify the changed value: \$ iqt -zp -fvalue LongParam where "name='cm.cm6compat'" value 0</pre>			

Appendix B. Increase Maximum Number of Open Files

The following procedure increases the maximum number of files that can be opened for reading and writing. As the number of servers in the topology grows, so does the need for additional files to handle merging data to the NOAM. This procedure checks the number of files currently in use, and, if necessary, increases the maximum number of open files.

Note: Following procedure is for one NOAM server. Repeat this procedure for other NOAM servers.

Procedure 43. Increase Maximum Number of Open Files

 Table 5. 2. Enter the following command to retrieve the pid of idbsvc. The highlighted in this sample output: \$ ps -ef grep -i idbsvc root 4369 idbsvc Up 03/0 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 3. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 2 in place of XXXX in the lsof' \$ sudo lsof -p XXXX wc -1 1278 4. Record the number of files currently open (the output of sub-step -1 5. Enter the following command to retrieve the pid of tpdProvd. Thighlighted in this sample output: \$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00 /usr/TKLC/plat/bin/tpdProvd 6. The number of open files is output with the 'lsof' command. Us 	ep#P	Procedure	Des	scription
number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for ass 1. Active NOAM CLI: Determine the number of files currently open 1. Use an SSH client to connect to the active NOAM. Ssh <noam address="" ip="" xmi=""> login as: admusr password: <enter password=""> Note: The static XMI IP address for each server should be a Table 5. 2. Enter the following command to retrieve the pid of idbsvc. The highlighted in this sample output: \$ ps -ef grep -i idbsvc root 4369 idbsvc Up 03/0 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 3. The number of open files is output with the 'Isof command. Up highlighted value from sub-step 2 in place of XXXX in the lsof \$ sudo lsof -p XXXX wc -1 1278 4. Record the number of files currently open (the output of sub-st \$ sudo lsof -p XXXX wc -1 1278 5. Enter the following command to retrieve the pid of tpdProvd. Thighlighted in this sample output: \$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00 /usr/TKLC/plat/bin/tpdProvd 6. The number of open files is output with the 'lsof command. Us highlighted value from sub-step 4 in place of XXXX in the lsof</enter></noam>			num	ber of files currently in use, and, if necessary, increases the maximum
 Active NOAM CL: Determine the number of files currently open Use an SSH client to connect to the active NOAM. ssh <noam address="" ip="" xmi=""> login as: admusr password: <enter password=""></enter></noam> Note: The static XMI IP address for each server should be a Table 5. Enter the following command to retrieve the pid of idbsvc. The highlighted in this sample output: \$ ps -ef grep -i idbsvc root 4369 idbsvc -MI0 -ME204 -D40 -DE820 -WI The number of open files is output with the 'lsof command. U: highlighted value from sub-step 2 in place of XXXX in the lsof \$ sudo lsof -p XXXX wc -1 1278 Record the number of files currently open (the output of sub-st ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00 /usr/TKLC/plat/bin/tpdProvd The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 4 in place of XXXX in the lsof 		(\mathbf{v}) each step as	it is	completed. Boxes have been provided for this purpose under each step
 CLI: Determine the number of files currently open Ssh <noam address="" ip="" xmi=""> login as: admusr password: <enter password=""></enter></noam> Note: The static XMI IP address for each server should be a Table 5. Enter the following command to retrieve the pid of idbsvc. The highlighted in this sample output: \$ ps -ef grep -i idbsvc root 4369 idbsvc - Up 03/0 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 The number of open files is output with the 'lsof' command. Up highlighted value from sub-step 2 in place of XXXX in the lsof \$ sudo lsof -p XXXX wc -1 1278 Record the number of files currently open (the output of sub-station) Enter the following command to retrieve the pid of tpdProvd. T highlighted in this sample output: \$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00 /usr/TKLC/plat/bin/tpdProvd The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 4 in place of XXXX in the lsof 	his proce	edure fails, it is r	recor	mmended to contact My Oracle Support (MOS) and ask for assistance.
 Determine the number of files currently open Note: The static XMI IP address> login as: admusr password: <enter password=""></enter> Note: The static XMI IP address for each server should be a Table 5. Enter the following command to retrieve the pid of idbsvc. The highlighted in this sample output: \$ ps -ef grep -i idbsvc root 4369 idbsvc Up 03/0 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 2 in place of XXXX in the lsof \$ sudo lsof -p XXXX wc -1 1278 Record the number of files currently open (the output of sub-step 2 in place of the output of sub-step 4 in place of the output of the ou	1. A	Active NOAM	1.	Use an SSH client to connect to the active NOAM.
number of files currently open login as: admusr password: <enter password=""> Note: The static XMI IP address for each server should be a Table 5. 2. Enter the following command to retrieve the pid of idbsvc. The highlighted in this sample output: \$ ps -ef grep -i idbsvc root 4369 idbsvc Up 03/0 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 3. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 2 in place of XXXX in the lsof' \$ sudo lsof -p XXXX wc -1 1278 4. Record the number of files currently open (the output of sub-st </enter>	-			ssh <noam address="" ip="" xmi=""></noam>
 Note: The static XMI IP address for each server should be a Table 5. 2. Enter the following command to retrieve the pid of idbsvc. The highlighted in this sample output: \$ ps -ef grep -i idbsvc root 4369 idbsvc Up 03/0 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 3. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 2 in place of XXXX in the lsof \$ sudo lsof -p XXXX wc -l 1278 4. Record the number of files currently open (the output of sub-stered the following command to retrieve the pid of tpdProvd. Thighlighted in this sample output: \$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00 //usr/TKLC/plat/bin/tpdProvd 6. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 4 in place of XXXX in the lsof formand. Us highlighted value from sub-step 4 in place of XXXX in the lsof formand. 				login as: admusr
 Table 5. 2. Enter the following command to retrieve the pid of idbsvc. The highlighted in this sample output: \$ ps -ef grep -i idbsvc root 4369 idbsvc Up 03/0 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 3. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 2 in place of XXXX in the lsof of \$ sudo lsof -p XXXX wc -1 1278 4. Record the number of files currently open (the output of sub-st 	C	currently open		password: <enter password=""></enter>
 highlighted in this sample output: \$ ps -ef grep -i idbsvc root 4369 idbsvc Up 03/0 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 3. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 2 in place of XXXX in the lsof' \$ sudo lsof -p XXXX wc -l 1278 4. Record the number of files currently open (the output of sub-stered subscription of the sub-stered subscription of the sub-stered subscription of the subscription of				<i>Note</i> : The static XMI IP address for each server should be available in Table 5.
 root 4369 idbsvc Up 03/0 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 3. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 2 in place of XXXX in the lsof' \$ sudo lsof -p XXXX wc -1 1278 4. Record the number of files currently open (the output of sub-stered) 5. Enter the following command to retrieve the pid of tpdProvd. Thighlighted in this sample output: \$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00 /usr/TKLC/plat/bin/tpdProvd 6. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 4 in place of XXXX in the lsof 			2.	Enter the following command to retrieve the pid of idbsvc. The pid is highlighted in this sample output:
 highlighted value from sub-step 2 in place of XXXX in the lsof \$				
 1278 4. Record the number of files currently open (the output of sub-state) 5. Enter the following command to retrieve the pid of tpdProvd. Thighlighted in this sample output: \$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00 /usr/TKLC/plat/bin/tpdProvd 6. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 4 in place of XXXX in the lsof 			3.	The number of open files is output with the 'lsof' command. Use the highlighted value from sub-step 2 in place of XXXX in the lsof command.
 5. Enter the following command to retrieve the pid of tpdProvd. Thighlighted in this sample output: \$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00 /usr/TKLC/plat/bin/tpdProvd 6. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 4 in place of XXXX in the lsof of the statement of the s				
 highlighted in this sample output: \$ ps -ef grep -i tpdProvd tpdProvd 347635 1 0 06:09 ? 00:00 /usr/TKLC/plat/bin/tpdProvd 6. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 4 in place of XXXX in the lsof to the second seco			4.	Record the number of files currently open (the output of sub-step 3):
 tpdProvd 347635 1 0 06:09 ? 00:00 /usr/TKLC/plat/bin/tpdProvd 6. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 4 in place of XXXX in the lsof 			5.	Enter the following command to retrieve the pid of tpdProvd. The pid is highlighted in this sample output:
 /usr/TKLC/plat/bin/tpdProvd 6. The number of open files is output with the 'lsof' command. Us highlighted value from sub-step 4 in place of XXXX in the lsof 				\$ ps -ef grep -i tpdProvd
highlighted value from sub-step 4 in place of XXXX in the lsof				
\$ sudo lsof -p XXXX wc -l			6.	The number of open files is output with the 'lsof' command. Use the highlighted value from sub-step 4 in place of XXXX in the lsof command.
1280				
			7.	Record the number of files currently open (the output of sub-step 5):

Step #	Procedure	Description
2.	Active NOAM CLI: Maximum number of open files	 Display the maximum number of open files for idbsvc. 8. Use the highlighted value from step 1, sub-step 2 in place of XXXX in the cat command. \$ sudo cat /proc/XXXX/limits grep -i open Max open files 32768 32768 files The output of the cat command displays the maximum number of files
		 that can be open by the idbsvc process. Record both values here: Soft Limit (1st value): Hard Limit (2nd value): This system has over 1024 open files, but its current ulimit for idbsvc is high enough during normal operation that the amount of open files does not pose a problem. However, when an attempt to upgrade another process (tpdProvd) updates idbsvc max # of open files to 1024, it causes the upgrade to fail. Display the maximum number of open files for tpdProvd. 9. Use the highlighted value from step 1, sub-step 4 for tpdProvd in place of
		 Solve the highlighted value hold only only out only hold only h
3.	Make sure the current number of open files used by idbsvc in in the safe limit	If the number of currently open files (step 1, sub-step 3) of idbsvc is less than the maximum allowed (step 2, sub-step 2 Soft Limit for tpdProvd), this procedure is complete, that is, number of currently open files (used by idbsvc) is less than 1024. Further steps are not required to be executed on this NOAM server. If the number of currently open files are more than the (step 2, sub-step 2 Soft Limit for tpdProvd), that is, 1024, go to step 5. Repeat this procedure (if required) for other NOAM server.
4.	Make sure the current number of open files used by tpdProvd in in the safe limit	If the maximum number of open files value (step 2, sub-step 2 - Soft Limit) for tpdProvd is already set to 32768, this procedure is complete. Further steps are not required to be executed on this NOAM server. If maximum value is not already set, then go to step 5. Repeat this procedure (if required) for other NOAM server.

Step #	Procedure	Description
5. □	Active NOAM CLI: Increase max number of	 Using a text editor with sudo, edit the file /etc/init/tpdProvd.conf to add these two lines just before the comment line in the file /etc/init/tpdProvd.conf that reads Start the daemon:
	open files	<pre># increase open file limit</pre>
		limit nofile 32768 32768
		Insight of file as example:
		<pre># # restart tpdProvd up to 10 times within a 100 second period. # If tpdProvd fails to start 10 times within a 100 second period then # it most likely has a deeper problem that restarting will not overcome. respawn limit 10 100</pre>
		<pre># increase open file limit limit nofile 32768 32768</pre>
		 Start the daemon script 2. Save the file and close the editor.
		Caution : Do not edit any other line in this file. You can back up the file, if required.
6.	Active NOAM CLI: Restart	1. Enter this command to stop tpdProvd:
		\$ sudo initctl stop tpdProvd
	tpdProvd service	2. Enter this command to restart tpdProvd:
		\$ sudo initctl start tpdProvd
		Sample output:
		tpdProvd start/running, proceed 186743
7.	Active NOAM CLI: Recheck	3. Enter the following command to retrieve the pid of idbsvc. The pid is highlighted in this sample output:
	open file maximum limit	\$ ps -ef grep -i idbsvc
		root <mark>8670</mark> idbsvc Up 03/01 13:03:28 1 idbsvc -M10 -ME204 -D40 -DE820 -W1 -S2
		 Use the highlighted value from sub-step 1in place of XXXX in the cat command.
		\$ sudo cat /proc/ <mark>XXXX</mark> /limits grep -i open
		Max open files 32768 32768 files
		 Verify the output of sub-step 2 indicates that the max number of open files is 32768. If the value is NOT 32768, it is recommended to contact My Oracle Support (MOS).

Appendix C. Upgrade Single Server – DSR 8.x

The following procedure upgrades a single DSR server of any type (NOAM, SOAM, MP, etc.) when the active NOAM is on DSR 8.x.

Note: This procedure may be executed multiple times during the overall upgrade, depending on the number of servers in the DSR and the chosen upgrade methodology. Make multiple copies of Appendix C to mark up, or keep another form of written record of the steps performed.

Procedure 44. U	Jpgrade Single Server –	- Upgrade A	Administration – DSR 8.x	(
-----------------	-------------------------	-------------	--------------------------	---

Step #	Procedure	Desci	ription					
This proc on releas	cedure executes t se 8.x.	he Upg	rade Single	Server – Up	grade Adm	inistration st	eps for a	an active NOAM
Check of number.	ff ($√$) each step as	s it is co	mpleted. Bo	oxes have b	een provide	ed for this pu	rpose u	nder each step
If this pro	ocedure fails, it is	recomn	nended to co	ontact My O	racle Suppo	ort (MOS) an	id ask fo	or assistance.
1.	Active NOAM VIP: View the pre-upgrade status of servers	2. N 3. S	Menu: Admini	dministratio	on > Softw ent of the se	are Manage erver to be up	ograded	Upgrade. (NOAM or site).
		NO_5 Host NO1 NO2	sg so_sg	Upgrade State Server Status Ready Norm Accept or Reject Err	OAM HA Role Appl HA Role Standby N/A Active N/A	Server Role Network Element Network OAM&P NO_DSR_VM Network OAM&P NO_DSR_VM	Function CAM&P CAM&P	Application Version Upgrade ISO 7.0.1.0.0-70.28.0 8.0.0.0.0-80.18.0
		Alarm	ctive NOAM 1 ID = 10008 1 ID = 32532	(Provision	ing Manua	lly Disabled	I)	cted alarms:
2 . □	Active NOAM VIP: Verify	1. Id	entify the se	rver to be u	pgraded (N			tc.) stname)
	status of server to be upgraded		erify the App lease versio		sion value i			,
			the server is ackup .	in the Bacl	kup Neede	d state, sele	ct the se	erver and click
		4. O	n the Upgrad	de Backup s	creen, click	KOK.		
		ТІ	he Upgrade	State chang	es to Back	up in Progr	ess.	
			erify the OAI ctive). This c					either standby or

Step #	Procedure	Description							
		Main Menu: Admi	nistration -> So	ftware Mana	gement -> Upg	rade	202		
		Filter* Tasks							
		NO_SG SO_SG							
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO		
		NO1	Backup Needed	Standby N/A	Network OAM&P	OAM&F	7.0.1.0.0-70.20.0		
		NO2	Accept or Reject		NO_DSR_VM Network OAM&P NO_DSR_VM	OAM&P	8.0.0.0.0-80.18.0		
		Backup Backup All 6. When the ba	Checkup Checkup	All Auto Upgra	de Accept Repo	oo <u>one/keess</u> e	nges to Ready .		
3. Active NOAM VIP: Initiate the server upgrade	VIP: Initiate the server	upgraded. 2. Click Upgra The Initiate I Main Menu: Admi	Jpgrade form	displays.			er to be		
		Filter* • Tasks •							
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Element	Function	Application Version Upgrade ISO		
		NO1	Ready	Standby N/A	Network GAM&P	OAMEP	7.0.1.0.0-70.28.0		
		NO2	Accept or Reject		Network OAM&P	OAM&P	8.0.0.0.0-80.18.0		
		Backup Backup All	Checkup Checkup	A Upgrade Se	rver coept Rep	port Report	t All		
4. Active NOAI VIP: Select upgrade ISO					ade ISO opti	ons, sel	ect the ISO to		
			e active NOA n HA switcho						
		the OAM backgro	I Max HA Ro und. This is l e user aware	le column c NOT an ala	displays Activ arm condition	ve with a . This in	dicator is to		
		2. Click OK.							
	1	The upgrade							

Step #	Procedure	Description						
		Main Menu: Ad	ministration ->	Software Ma	nagement ->	Upgrade [
		Info* 👻					- Mon Dec 26 2	
		Hostname Action		Statu	s			
		NO1 Upgra	de	OAM		twork Element	Application Version 7.0.1.0.0-70.28.0	
		Upgrade Settings						
		Upgrade ISO DSR-	8.0.0.0.0_80.18.0-x86	5_64 iso 🔽 Selec	t the desired upgrad	ie ISO media file.		
		Ok Cancel						
		NOAM via	f the GUI, cle	ear the bro	wser cach uing. Som	e GUI fo	g back into the active rms may exhibit ed.	
5.	Active NOAM VIP: View the upgrade administration form to monitor upgrade progress	ROLL Upgra The e in the 1. Observe t screen by	ar instructions upgrade pro BACK to the ade displays execution tim upgrade whe selecting the	s if the upg cessing en e original s as FAILEI e may be s ere there v status of th e Entire S i	rade fails. counters a oftware re D. shorter or l vas a prob ne site on t i te link. A	a problem lease. In onger, de lem. he Upgra	le progress. n, it may attempt to n this case, the epending on the point ade Administration e status summary of Upgrade States	
		Main Menu: Adn	ninistration -> S	oftware Mana	gement -> U	pgrade	Mon Dec 25 22:2	
		Filter* • Status	• Tasks •				300 Dec 29 4212	
		NO_5G 90_96					And the second	
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role	Server Role Network Eleme	Function	Application Version Upgrade ISO	
		NO1	Upgrading	Standby	Network OAM&		7.0.1.0.0-70.28.0	
			Warn Accept or Rejec	N/A Actor	NO_DSR_VM Network OAM88	CAMAP	DSR-8.0.0.0.0_80.18.0-x86_64.80 8.0.0.0-60.18.0	
		NO2	En	N/A	NO_DER_VM	Crime	00.000.000	
		Alarn Alarn becai Alarn Alarn Alarn	ll servers ha n ID = 10008 n ID = 10075 use applicat n ID = 10073 n ID = 32515 n ID = 31228	ve all alarm (Provisio (The serv tion proce (Server G (Server H (HA High	ns: ver is no lo sses have froup Max IA Failove Iy availab	ually Dis onger pro been m Allowed r Inhibite le server	abled) oviding services anually stopped) d HA Role Warning)	

Step #	Procedure	Description
		Alarm ID = 31283 (Highly available server failed to receive mate heartbeats)
		Alarm ID = 31106 (DB Merge To Parent Failure)
		Alarm ID = 31107 (DB Merge From Child Failure)
		Alarm ID = 31233 (HA Secondary Path Down)
		Alarm ID = 31101 (DB Replication To Slave Failure)
		Alarm ID = 31104 (DB Replication over SOAP has failed
		Alarm ID = 31282 (The HA manager (cmha) is impaired by a s/w fault)
		Alarm ID = 31225 (HA Service Start Failure)
		Alarm ID = 31226 (HA Availability Status Degraded)
		Alarm ID = 31114 (DB Replication over SOAP has failed)
		Alarm ID = 31149 (DB Late Write Nonactive)
		 Wait for the upgrade to complete. The Status Message column displays Success. This step takes approximately 20 to 50 minutes.
		<i>Note</i> : In the unlikely event that after the upgrade, if the Upgrade State of server is Backout Ready or Failed and the Status Message displays Server could not restart the application to complete the upgrade , then perform Appendix M Manual Completion of Server Upgrade to restore the server to full operational status and return to this step to continue the upgrade.
		Perform Appendix U to create a link of Comagent.
		If the upgrade fails, do not proceed . It is recommended to consult with Appendix U on the best course of action. Refer to Appendix I for failed server recovery procedures.

Step #	Procedure	Description
6.	Server CLI:	An optional method to view Upgrade progress from the command line:
	(Optional) View	To view the detailed progress of the upgrade , access the server command line (via SSH or Console), and enter:
	in-progress status from	<pre>\$ tail -f /var/TKLC/log/upgrade/upgrade.log</pre>
	command line of server	This command displays the upgrade log entries as the events occur. Once the upgrade is complete, the server reboots. It takes a couple of minutes for the DSR application processes to start up.
		For example, this command displays the current rev on the server:
		[admusr@NO2 ~]\$ appRev
		Install Time: Thu Dec 15 00:05:46 2016
		Product Name: DSR
		Product Release: 8.6.0.0.0_95.14.0
		Base Distro Product: TPD
		Base Distro Release: 7.7.0.0.0-88.68.0
		Base Distro ISO: TPD.install-7.7.0.0.0_88.68.0- OracleLinux6.10-x86_64.iso
		ISO name: DSR-8.6.0.0.0_95.14.0-x86_64.iso
		OS: OracleLinux 6.10
		If the upgrade fails, do not proceed . It is recommended to consult with on the best course of action. Refer to Appendix I for failed server recovery procedures.
7 .	Server CLI: If the upgrade fails	If the upgrade of a server fails, access the server command line (via ssh or a console), and collect the following files:
	Tullo	/var/TKLC/log/upgrade/upgrade.log
		/var/TKLC/log/upgrade/ugwrap.log
		/var/TKLC/log/upgrade/earlyChecks.log
		/var/TKLC/log/platcfg/upgrade.log
		It is recommended to contact My Oracle Support (MOS) by referring to Appendix U of this document and provide these files. Refer to Appendix I for failed server recovery procedures.

Step #	Procedure	Description						
8.	Active NOAM VIP: Verify post upgrade status	 Navigate to Administration > Software Management > Upgrade. Select the tab of the NOAM or site being upgraded. Verify the Application Version value for this server has been updated to the target software release version. Verify the Upgrade State of the upgraded server is Accept or Reject. Main Menu: Administration -> Software Management -> Upgrade Filler = Status = Tests						
9.	Active NOAM/SOAM VIP: Verify the server was successfully upgraded	Entry Sin SOL Lest IPFE_SO MPFE_SO SSTWP_SO1 Hostname Server Status Appl HA Role Server Role Panction Application Version S01 Accept or Fleet NA So1_DSR_VM DSR-R020.80.17.0 B00.90.17.0 S02 Accept or Reject NA So1_DSR_VM DSR-R020.0_0.80.17.0 B00.00.90.17.0 S02 Accept or Reject Standby Byten OAM B00.00.90.17.0 B00.00.90.17.0 S02 Accept or Reject NA So1_DSR_VM DSR-R020.0_0.80.17.0 B00.0.90.17.0 S02 Accept or Reject Standby Byten OAM B00.0.00.0_0.0.17.0 B00.0.00.0_0.0.17.0 S02 Accept or Reject Standby Byten OAM B00.0.00.0_0.0.17.0 B00.0.00.0_0.0.17.0 S02 Accept or Reject NA So1_DSR_VM DSR-R0.00.0_0.0.17.0 B00.0.00.0_0.0.17.0 S03 Accept or Reject NA So1_DSR_VM DSR-R0.00.0_0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.						
		The active NOAM or SOAM has these expected alarms until both NOAMs/SOAMs are upgraded: Alarm ID = 31233 – HA Secondary Path Down Alarm ID = 32532 (Server Upgrade Pending Accept/Reject) Note: Do not accept upgrade at this time. This alarm is OK.						

Appendix D. Upgrade Multiple Servers – Upgrade Administration

The following procedure upgrades multiple servers in parallel.

Note: This procedure is executed multiple times during the overall upgrade, depending on the number of servers in your DSR. Make multiple copies of Appendix D to mark up or keep another form of written record of the steps performed.

Procedure 45. Upgrade Multiple Servers – Upgrade Administration

Step #	Procedure	Description	Description						
This proc	cedure executes t	he Upgrade Mu	Itiple Servers	s – Upgrade	e Adminis	stration st	eps.		
Check of number.	f (\checkmark) each step as	s it is completed	I. Boxes have	e been prov	vided for	this purpo	ose under each step		
f this pro	ocedure fails, it is	recommended	to contact My	/ Oracle Su	ipport (M	OS) and a	ask for assistance.		
1.	Active NOAM	1. Log into t	he NOAM GL	JI using the	VIP.				
	VIP: View pre-upgrade	2. Navigate	to Administr	ation > So	ftware N	lanagemo	ent > Upgrade.		
	status of the servers	The active alarms:	e NOAM serv	er may hav	/e some	or all of th	e following expected		
		Alarm ID	= 10008 (Pro	ovisioning	Manuall	y Disable	ed)		
			= 32532 (Se			•	pt/Reject)		
		Main Menu: Adn	ninistration -> S	oftware Man	agement -:	> Upgrade			
		Filter . Tasks	•						
		Filter • Tasks		SBR_SQ_A GTF	(SBR_SG_B	GTR_SO_SG	HSUPPELA INSUPPELB 1		
		Party management of the second		SBR_SG_A OTF OAM Max HA Role	Description for the Land	GTR_SO_SG Function	NSCIPFE_A NSCIPFE_B 1 Application Version		
		Party management of the second	GTR_MP_SG GTR	and reaction of a reaction	Description for the Land	Function			
			GTR_MP_SG CTR_ Upgrade State	OAll Max HA Role Max Allowed	Server Role	Function	Application Version		
		Kostname GTR-MP-01	GTR_MP_SG CTR_ Upgrade State	OAll Max HA Role Max Allowed HA Role	Server Role Network Eleme	Function Int DSR (multi- active duster) E DSR (multi- active	Application Version Upgrade (SO		
		Nestname	GTR_MP_SG CTR_ Upgrade Statu Server Status	OAN Max HA Role Max Allowed HA Role Spare Active	Server Role Network Eleme MP GTR_SOAN_NE	Function nt DSR (multi- active duster) E DSR (multi- active duster)	Application Version Upgrade ISO 7.0.0.0.0-70.7.0		
		Kostname GTR-MP-01	GTR_MP_SG CTR_ Upgrade Statu Server Status Coccup Mended Auron	OAM Max HA Role Max Allowed HA Role Spare Active Spare	Server Role Network Eleme MP GTR_SOAM_NE MP	Function nt DSR (multi- active duster) E DSR (multi- active duster)	Application Version Upgrade ISO 7.0.0.0.0-70.7.0		
		Kostname GTR-MP-01 GTR-MP-02	GTR_MP_SG CTR_ Upgrade Statu Server Status Coccup Mended Auron	OAM Max HA Role Max Allowed HA Role Spare Active Spare Active	Server Role Network Eleme MP GTR_SOAW_NE GTR_SOAW_NE	Function Turnetion DSR (multi- active duater) DSR (multi- active duater) DSR (multi- active duater)	Application Version Upgrade ISO 7.0.00.0-70.7.0 7.0.00.0-70.7.0		

Step #	Procedure	Description					
2.	Active NOAM VIP: Verify	1. Identify the N	/IP servers to		d in parallel rd names)		
	status of servers to be upgraded	2. Verify the Ap release version	•		•		e software
		3. Navigate to a select the Se			-	ment > l	Upgrade and
		Main Menu: Admir	nistration -> So	ftware Manag	ement -> Upgr	ade	
		Filter* • Tasks •					
		BarrA_BINDING_SO E	amA_MP_SO BarrA	_so_sg _gtxa_)	IP_SG GTXA_NO	SG OTXA_	SESSION_SG
		Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version
			Server Status	Appl HA Role	Network Element		Upgrade ISO
		BarrA-SO-SP	Backup Needed	Standby		CAM	7.3.0.0.0-73.14.0
		BarrA-SO1	Backup Needed	Active	BarracudaA_111120 System OAM	OAM	7.3.0.0.0-73.14.0
		Backup Backup All	Norm Checkup Checkup	N/A All Auto Upgrade	BarracudaA_111120		3
		succup succup an	checkap checkap	na reas spyrios	Manual Contractor	reporten	8
		is complete,	e State chang the Upgrade AM Max HA I	es to Back i State chang Role is in th	up in Progre les to Ready e expected c	ess. Wh r. condition	s and click hen the backup (either standb

Step #	Procedure	Description						
3.	Active NOAM VIP: Verify	The Upgrade Ad displays Upgrad					ograde	
	upgrade	Main Menu: Administration -> Software Management -> Upgrade						
	status is Ready	Filter* • Tasks* •						
		BarrA_BINDING_SG	BanA_MP_SG Ban	A_50_56 GTXA_	MP_SG GTXA_NO	_sg gtxa	SESSION_SG	
		Hostname	Upgrade State Server Status	OAM HA Role	Server Role Network Element	Function	Application Version Upgrade ISO	
		BarrA-SO-SP	Ready	Standby	System OAM BarracudaA_111120	CAM	7.3.0.0.0-73.14.0	
		BarrA-SO1	Ready	Active NIA	System OAM BarracudaA_111120	OAM	7.3.0.0.0-73.14.0	
		Backup Backup All	Checkup Checku				7	
		Alarm II Alarm II because Alarm II Alarm II Alarm II Alarm II Alarm II Alarm II Alarm II	D = 10075 (The application D = 32515 (Solution D = 31101 (D D = 31106 (D D = 31107 (D D = 31228 (Here eartbeats) or D = 31114 (D D = 31225 (Here	erver Group ne server is processes erver HA Fa B Replicatio B Merge to I B Merge Fro A Highly ava (Lost Comn B Replicatio A Service Se	Max Allowe no longer p have been r ilover Inhibi on to slave D Parent Failu om Child Fai ailable serve nunication w on over SOA tart Failure)	ed HA Ro roviding nanually ted) 9B has fa re) lure) er failed vith Mate P has fa	v stopped) ailed) to receive e Server) iled)	
4. □	Determine upgrade method – manual or automatic	To upgrade mult steps 5. and 6. To upgrade a se option, proceed	erver group us	•	0	•		

	Procedure	Description								
5. Active NOAM VIP: Initiate upgrade (part	VIP: Initiate	 From the U Click Upgra 	. •	nistration scr	een, select tł	ne servei	rs to upgrade.			
	1)	Main Menu: Adm	Main Menu: Administration -> Software Management -> Upgrade							
		Filter* • Tasks •								
		BarrA_BINDING_SG	BarrA_MP_\$G Ba	na_so_so gtxa	JMP_SG GTXA_N	D_SG GTXA	_SESSION_80			
		Hostname	Upgrade State	OAM HA Role	Server Role	Function	Application Version			
		nosenne	Server Status	Appl HA Role	Network Element		Upgrade ISO			
		BarrA-MP1	Ready	Standby	MP	DISFR (multi- active cluster)	7.3.0 0.0-73.14.0			
			Neorm	Active	BarracudaA_11112	01_90				
		BarrA-MP2	Ready	Active	MP	DISR (multi- active cluster)	7.3.0.0.0-73.14.0			
			Nom	Active	BarracudaA_11112	01_90				
6.	Active NOAM VIP: Initiate upgrade (part	1. From the U use in the s	pgrade Settin erver upgrade	e Initiate scr ngs – Upgra	een.		> Software			
6.		 From the U use in the s Click OK. 	ent > Upgrade pgrade Settir	e Initiate scr ngs – Upgra e.	een. I de ISO optio	ons, sele	ct the ISO to			
6.	VIP: Initiate upgrade (part 2) – Select	 From the U use in the s Click OK. The upgrad 	ent > Upgrade pgrade Settin erver upgrade e begins and	e Initiate scr ngs – Upgra e. control retur	een. I de ISO option	ons, sele grade Ac	ct the ISO to			
6.	VIP: Initiate upgrade (part 2) – Select	 From the U use in the s Click OK. The upgrad screen. 	ent > Upgrade pgrade Settin erver upgrade e begins and	e Initiate scr ngs – Upgra e. control retur	een. I de ISO option	ons, sele grade Ac	ct the ISO to			
6.	VIP: Initiate upgrade (part 2) – Select	 From the U use in the s Click OK. The upgrad screen. Main Menu: Adm 	ent > Upgrade pgrade Settin erver upgrade e begins and	e Initiate scr ngs – Upgra e. control retur	een. I de ISO option	ons, sele grade Ac	ct the ISO to			
6.	VIP: Initiate upgrade (part 2) – Select	 From the U use in the s Click OK. The upgrad screen. Main Menu: Adm 	ent > Upgrade pgrade Settin erver upgrade e begins and	e Initiate scr ngs – Upgra e. control retur	een. Ide ISO option Ins to the Upper	ons, selec grade Ac de [initiat	ct the ISO to			
6.	VIP: Initiate upgrade (part 2) – Select	 From the U use in the s Click OK. The upgrad screen. Main Menu: Adm Hostname Action 	ent > Upgrade pgrade Settin erver upgrade e begins and inistration -> So	e Initiate scr ngs – Upgra e. control retur ftware Manag Status OAM HA R	een. de ISO optic ns to the Up ement -> Upgra de Appl HA Bo Active	ons, seler grade Ac ide [initiat de Neth Barn de Neth	ct the ISO to Iministration e] work Element acudaA_1111201_50 work Element			
6.	VIP: Initiate upgrade (part 2) – Select	 From the U use in the s Click OK. The upgrad screen. Main Menu: Adm Intervention BarrA-MP1 Upgrade BarrA-MP2 Upgrade 	ent > Upgrade pgrade Settin erver upgrade e begins and inistration -> So	e Initiate scr ngs – Upgra control retur oftware Manago Status OAM HA R Standby	een. de ISO optic ns to the Up ement -> Upgra de Appl HA Bo Active	ons, seler grade Ac ide [initiat de Neth Barn de Neth	ct the ISO to Iministration e] work Element acudaA_1111201_50			
6.	VIP: Initiate upgrade (part 2) – Select	 From the U use in the s Click OK. The upgrad screen. Main Menu: Adm Hostname Action BarrA-MP1 Upgrade 	ent > Upgrade pgrade Settin erver upgrade le begins and inistration -> So	e Initiate scr ngs – Upgra control retur oftware Manag Status OAM HA R Standby OAM HA R RESUM	een. de ISO optic ns to the Up ement -> Upgra de Appl HA Ro Active	ons, seler grade Ac ide [initiat ie Neh Barn ie Neh Barn	ct the ISO to Iministration e] work Element acudaA_1111201_50 work Element			
6.	VIP: Initiate upgrade (part 2) – Select	 From the U use in the s Click OK. The upgrad screen. Main Menu: Adm More Action BarrA-MP1 Upgrade BarrA-MP1 Upgrade BarrA-MP2 Upgrade 	ent > Upgrade pgrade Settin erver upgrade le begins and inistration -> So	e Initiate scr ngs – Upgra control retur oftware Manag Status OAM HA R Standby OAM HA R RESUM	een. de ISO optic ns to the Up ement -> Upgra de Appl HA Ro Active	ons, seler grade Ac ide [initiat ie Neh Barn ie Neh Barn	ct the ISO to Iministration e] work Element acudaA_1111201_50 work Element			

Step #	Procedure	Description	
7.	Active NOAM VIP: Initiate	 To utilize the Automated Server Group upgrade option in the server group are selected. 	, verify no servers
	(part 1) – Automated	Main Menu: Administration -> Software Management -> Upgrade	
	Server Group	Filter* + Tasks +	
	Upgrade option	BarrA_BINDING_SG BarrA_MP_SG BarrA_SO_SG GTXA_MP_SG GTXA_NO_SG B	STXA_BESSION_SG
	-	Hostname Upgrade State OAM HA Role Server Role Function	n Application Version
		Server Status Appl HA Role Network Element	Upgrade 150
		BarrA-MP1 Ready Standby MP active cluster)	7.3.0.0.0-73.14.0
		Norm Active BarracudaA_1111201_SO	
		BanA-MP2 Ready Active MP active cluster)	7.3.0.0.0-73.14.0
		Norm Active BarracudaA_1111201_SO	
		Backup Backup All Checkup Checkup All Auto Upgrade Accept Report Report	ortAll
		2. Click Auto Upgrade.	

Step #	Procedure	Description							
8. □	Active NOAM VIP: Initiate	<i>Note</i> : The settings to be used in this step are specified in the calling procedure.							
	(part 2) – Automated Server Group Upgrade	1. The Upgrade Settings section of the Initiate screen controls the behavior of the automated upgrade. Select the settings that apply to the server type being upgraded.							
		Bulk : Select this option for active/standby and multi-active server groups. For servers in an active/standby configuration, the standby server is upgraded first, followed by the active. Servers in a multi-active configuration are upgraded in parallel to the extent allowed by the Availability setting.							
		Seria	I: Select this option to u	pgrade mul	tiple servers	one at a time.			
		Grou	ped Bulk: Select this or /s upgrades the spare(s	ption for SB	R server gro	ups. Grouped bulk			
		Availability : This setting determines how many servers remain in service while servers in the server group are upgraded. For example, a setting of 50% ensures at least half of the servers in the server group remain in service.							
		2. Selec							
		Main Men	u: Administration -> Softwa	re Manageme	nt -> Upgrade	[Initiate]			
		into" +							
		Hostname	Action	Status					
		BarrA-MP1	Auto upgrade	OAM HA Role	Appl HA Role	Network Element			
				Standby	Active	BarratudaA_1111201_80			
		and the second second		OAM HA Role	Appl HA Role	Network Element			
		BarrA-MP2	Auto upgrade	Active	Active	BarratudaA_1111201_50			
		Upgrade Settings							
		-		Server group upgra					
		Mode	 Bulk Genued Bulk 	Select "Bulk" to upgrade servers in groups according to the available Select "Senal" to upgrade servers one at a time in HA order. Select "Grouped Bulk" to upgrade servers in HA groups according to in all modes, any designated last server will be upgraded last. HA groups are created according to the "Application HA Role" of the The HA role order is spare, observer, standby and active.					
		Availability	ervers in the server group during b will be unavailable.)						
				DISCOUNT AND ADDRESS		11 (* 1778 * 1777 5 0 (* 1797 17 17 17 17 17 17 17 17 17 17 17 17 17			
		Upgrade ISO	DSR-8.0.0.0.0_80.13.0-x86_64.iso •	Select the desired u	opgrade ISO media file				

Step #	Procedure	Description					
9.	Active NOAM VIP: View the upgrade administration form to monitor upgrade progress	 See step 10. for an optional method of monitoring upgrade progress. See step 11. for instructions if the Upgrade fails, or if execution time exceeds 60 minutes. <i>Note</i>: If the upgrade processing encounters a problem, it may attempt to ROLL BACK to the original software release. In this case, the Upgrade displays as FAILED. The execution time may be shorter or longer, depending on the point in the upgrade where there was a problem. 1. Observe the upgrade status of the servers of interest. Upgrade status displays under the Status Message column. 					
					gement -> Upgra	de	-
		Filter* Status BartA_BINDINO_SO	BarrA MP 515 88	NA SO SO OTXA	MP Số (UTXA NO B	a atxa	SESSION_SO OTXA_SO_BO
		Hostname	Upgrade State Server Status	OAM HA Role Appl HA Role		Function	Application Version Upgrade ISO
		BarrA-MP1	Pending	Active	MP a	DSR (multi- ictive luster)	7.3.0.0.0-73.14.0
		BarrA-MP2	Upgrading	Active 005	MP a	SO OSR (multi- ictive (uster)	DSR-6.0.0.0.0_80 13.0-x86_64 iso
			Unik	NA	Barracuda4_1111201_		DSR-8.0.0.0_50 13.0-x86_64 iso
			ll servers ha D ID = 10008			lv Dis	abled)
		Alarn Alarn becar Alarn Alarn Alarn Alarn Mate Alarn Alarn Alarn heart Alarn	h ID = 10008 $h ID = 10073$ $h ID = 10075$ $use application ID = 31101$ $h ID = 31106$ $h ID = 31228$ $heartbeats)$ $h ID = 31283$ $heats)$ $h ID = 32515$	G (Provision G (Server G G (The server Con process (DB Replin G (DB Merg G (DB Merg G (HA Highl or (Lost C G (HA Seco G (Highly av G (Server H	ning Manual roup Max Al er is no long sses have be ication To Sl e To Parent e From Child ly available s Communicati ndary Path I vailable serv A Failover In	lowed ger pro- een m ave F Failur d Failu server ion wi Down) er fail	d HA Role Warning) oviding services anually stopped) ailure) re) ure) failed to receive th Mate Server) ed to receive mate
		Success When an displays t This alarn	This step ta upgraded S(o alert the op n is active ur = 25607 (DS	akes appro DAM becor perator to e ntil the firew	ximately 20 to nes active on	o 50 m relea: w Sign d in Pr	inutes. se 8.x, Alarm 25607 aling Firewall feature. ocedure 27.

Step #	Procedure	Description
		If the upgrade fails – do not proceed. It is recommended to consult with on the best course of action. Refer to Appendix I for failed server recovery procedures.
10.	Server CLI: (Optional) View in- progress status from command line	Optional method to view upgrade progress from a command line: To view the detailed progress of the upgrade – Access the server command line (via ssh or Console), and: \$ tail -f /var/TKLC/log/upgrade/upgrade.log Once a server is upgraded, it reboots, and it takes a couple of minutes for the DSR application processes to start up. This command displays the current rev on the upgraded servers: [admusr@NO1 ~]\$ appRev Install Time: Wed Apr 4 05:03:13 2018 Product Name: DSR Product Release: 8.6.0.0.0_95.14.0 Base Distro Product: TPD Base Distro Release: 7.7.0.0.0-88.68.0 Base Distro ISO: TPD.install-7.7.0.0.0_88.68.0- OracleLinux6.10-x86_64.iso OS: OracleLinux 6.10 If the upgrade fails, do not proceed . It is recommended to consult with on the best course of action. Refer to Appendix I for failed server recovery procedures.
11.	Server CLI: If upgrade fails	If a server upgrade fails, access the server command line (via ssh or Console), and collect the following files: /var/TKLC/log/upgrade/upgrade.log /var/TKLC/log/upgrade/ugwrap.log /var/TKLC/log/upgrade/earlyChecks.log /var/TKLC/log/platcfg/upgrade.log If the upgrade fails, do not proceed . It is recommended to consult with on the best course of action. Refer to Appendix I for failed server recovery procedures.
12.	Active NOAM VIP: Verify post upgrade status	 Navigate to Administration > Software Management > Upgrade. Verify the Application Version value for the servers has been updated to the target software release version. Verify the Status Message indicates success. Verify the Upgrade State of the upgraded servers is Accept or Reject.

Step #	Procedure	Description
13.	Verify the servers were successfully upgraded	 View Post-Upgrade Status of the server: The active SOAM server may have some or all the following expected alarm(s): Alarm ID = 10008 (Provisioning Manually Disabled) Alarm ID = 10010 (Stateful database not yet synchronized with mate database) Alarm ID = 10075 (The server is no longer providing services because application processes have been manually stopped) Alarm ID = 31000 (Program impaired by S/W Fault) Alarm ID = 32532 (Server Upgrade Pending Accept/Reject) Note: Do not accept upgrade at this time. This alarm is OK.

Appendix E. IDIH Upgrade at a Site

In IDIH release 7.1 and later, the mediation and application instance data is stored in the Oracle Database. This allows the Application and Mediation servers to be upgraded by performing a fresh installation. Upon completion of the upgrade, the mediation and application guests automatically restore the configuration data from the Oracle database.

Table 24 shows the elapsed time estimates for IDIH upgrade.

	Elapsed Time (hr:min)			
Procedure	This Step	Cum.	Procedure Title	Impact
Procedure 46	1:15-1:45	1:15-1:45	Procedure 46	None
Procedure 47	0:30-0:45	1:45-2:30	Procedure 47	None

Appendix E.1. Upgrade Oracle Guest

The Oracle Guest is upgraded first.

Procedure 46. Upgrade Oracle Guest

Step #	Procedure	Description			
This proc	This procedure performs the IDIH Oracle Guest upgrade.				
number.	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				
		econimended to contact my Oracle Support (mOS) and ask for assistance.			
1.	IDIH CLI:	1. Log into the Oracle guest as the admusr user.			
	Perform a system health	ssh <idih address="" ip=""></idih>			
	check on the	login as: admusr			
	Oracle guest	password: <enter password=""></enter>			
		2. Execute the analyze_server.sh script.			
		<pre>\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</pre>			
		Sample output:			
		[admusr@cat-ora ~]\$ /usr/TKLC/xIH/plat/bin/analyze_server.sh -i			
		13:24:52: STARTING HEALTHCHECK PROCEDURE			
		13:24:52: date: 03-17-15, hostname: cat-ora			
		13:24:52: TPD VERSION: 7.0.0.0.0-86.14.0			
		13:24:52:			
		13:24:52: Checking disk free space			
		13:24:52: No disk space issues found			
		:			
		13:25:02: All tests passed!			
		13:25:02: ENDING HEALTHCHECK PROCEDURE WITH CODE 0			
		If the output indicates the following error, ignore the error and continue the upgrade. This error indicates the target release and the running release are the same.			
		00:47:29: Checking runlevel			
		00:47:29: >>> Error: Runlevel value "3 4" is different from "N 4"			
		If the output indicates any other failure, do not proceed with the upgrade. It is recommended to contact My Oracle Support (MOS) for guidance.			

Step #	Procedure	Description		
2.	IDIH CLI:	1.	Log into the Mediation guest as admusr user.	
	Shut down the Mediation		ssh <idih address="" ip=""></idih>	
	guest to		login as: admusr	
	prepare for the		password: <enter password=""></enter>	
	Oracle guest upgrade	2.	Shut down the Mediation guest.	
	apgrade		\$ sudo init 0	
			The active SOAM server may have some or all of the following expected alarms:	
			Alarm ID = 19800 Communication Agent Connection Down	
			Alarm ID = 11511 Unable to connect via Comagent to remote DIH server with hostname	
			The active NOAM server may have some or all of the following expected alarms:	
			Alarm ID = 19800 Communication Agent Connection Down	
3.	IDIH CLI:	1.	Log into the Application guest as admusr user.	
	Shut down the Application		ssh <idih address="" ip=""></idih>	
	guest to		login as: admusr	
	prepare for the		password: <enter password=""></enter>	
	Oracle guest upgrade	2.	Shut down the Application guest.	
	upgrade		\$ sudo init 0	
			The active SOAM server may have some or all of the following expected alarms:	
			Alarm ID = 19800 Communication Agent Connection Down	
			Alarm ID = 11511 Unable to connect via Comagent to remote DIH server with hostname	
			The active NOAM server may have some or all of the following expected alarms:	
			Alarm ID = 19800 Communication Agent Connection Down	

Step #	Procedure	Description
4.	IDIH Application Guest CLI:	 It is seen that space available in /var/TKLC directory is less than the ISO size. So, there is need to increase the space of this directory.
		2. Log into the Application guest as admusr user.
	Increase Size of /var/TKLC	ssh <idih address="" ip=""></idih>
		login as: admusr
		password: <enter password=""></enter>
		3. Check the space
		df -kh /var/TKLC
		 Note down the current space. Available space should be more than 6 GB space for this. In case sufficient space is already there, skip next sub- steps.
		5. Increase the space
		<pre>sudo lvresize -L +6G /dev/mapper/vgroot-plat_var_tklc</pre>
		6. Resize the space
		<pre>sudo resize2fs /dev/mapper/vgroot-plat_var_tklc</pre>
		7. Check the space again
		df -kh /var/TKLC
		8. Available space should be more than 6 GB space for this.
5.	Move Oracle ISO	Use a file transfer tool to copy the Oracle ISO to the Oracle guest as admusr. Example:
		\$ scp oracle-DSR-8.6.0.0.0 95.14.0-x86 64.iso
		admusr@ <ora-guest-ip>:/var/TKLC/upgrade</ora-guest-ip>
6.	IDIH CLI:	The Oracle guest is upgraded using the Platform Configuration utility.
	Start Oracle guest upgrade	1. Launch the platform configuration utility.
		\$ sudo su - platcfg
		 In the resulting menu, navigate to Maintenance > Upgrade > Initiate Upgrade.
		 At the ISO selection menu, select the target release Oracle ISO and press Enter.
		Choose Upgrade Media Menu oracle-7.2.0.0.0_72.19.0-x86_64.iso - 7.2.0.0.0_72.19.0 ê Exit

Step #	Procedure	Description
7.	IDIH CLI: Monitor upgrade progress	The platform configuration menu exits and the guest reboots when the upgrade completes. To view the detailed progress of the upgrade, access the server command line (via SSH or Console), and enter: \$ tail -f /var/TKLC/log/upgrade/upgrade.log Once the server has upgraded, it reboots. It takes a couple of minutes for the Oracle processes to start up.
		Note: The iso file for DB upgrade contains the default ASMSetup file and it is possible for it to overwrite "sd" definition with vd for disks. This affects the upgrade on setups that has sd disks, like sda, sdb and so on. In this scenario, just after the upgrade, when a reboot is triggered, it is possible that ASM will not be able to assign sdb disk to be used for Oracle DB. This can be verified by checking /etc/udev/rules.d/98-asm.rules file. This would contain KERNEL=="dm-7" SYMLINK+="asm/ASM0" OWNER="grid" GROUP="oinstall" MODE="0660" entry and KERNEL=="sdb" SYMLINK+="asm/ASM1" OWNER="grid" GROUP="oinstall" MODE="0660" would be removed. If sdb is missing from this file, it is recommended to edit ASMSteup file, \$sudo vi /opt/xIH/oracle/instances/ASMSetup. Locate line 94, modify the expression ^vd by ^sd and save the file. Reboot the VM achange after making the changes. This would resolve the problem.
8.	IDIH CLI: Perform a system health check on the Oregin quest	 Wait a few minutes to allow the Oracle guest to stabilize after the reboot, and repeat step 1 to perform the post-upgrade system health check. <i>Note</i>: The following warnings are expected due to the mediation and app servers being shut down.
	Oracle guest	Warning: mediation server is not reachable (or ping response exceeds 3 seconds)
		Warning: app server is not reachable (or ping response exceeds 3 seconds)

Appendix E.2. Upgrade the Mediation and Application Guests

The Mediation and Application Guest upgrade is similar to the installation procedure.

Procedure 47. Upgrade the Mediation and Application Guests

Step #	Procedure	Description	
This proc	edure performs th	ne IDIH Mediation and Application server upgrade.	
Check of number.	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.		
If this pro	ocedure fails, it is r	ecommended to contact My Oracle Support (MOS) and ask for assistance.	
1. CLOUD GUI: Remove existing Application Server Use the hypervisor-specific procedure to remove the current iDIH and iDIH Mediation guests.		Use the hypervisor-specific procedure to remove the current iDIH Application and iDIH Mediation guests.	

Step #	Procedure	Description
2.	CLOUD GUI : Deploy the latest application and mediation guest images	Use the hypervisor-specific procedure to deploy the latest Application and Mediation guests. Configure the iDIH mediation and application guests to reflect the guest profile in the installation document [1].
3.	IDIH CLI: Configure the IDIH VM Networks	Configure the iDIH mediation and application guests according to Procedure 32 (Configure iDIH Virtual Machines) of installation document [1].
4.	IDIH CLI: Run Post Installation scripts on iDIH VMs	Execute Post Installation iDIH mediation and application specific scripts on the respective iDIH guests according to Procedure 33 (Run Post Installation scripts on iDIH VMs) of installation document [1].
5.	NOAM CLI: Reset SOAP password	In case upgrading to release IDIH 8.2.3, reset the SOAP password to allow self-authentication of DSR with IDIH to send traces. Refer to the Appendix Reset the SOAP Password.

Appendix F. Alternate Server Upgrade Procedures

The following procedure provides alternative ways of upgrading various server types, using an array of differing methods. All of the procedures in this section are secondary to the upgrade methods provided in Section 4 and Section 5. These procedures should be used only when directed by or by other procedures within this document.

Appendix F.1. Alternate Pre-Upgrade Backup

The following procedure is an alternative to the normal pre-upgrade backup provided in Procedure 14. It is recommended that this procedure be executed only under the direction of .

Procedure 48. Alternate Pre-Upgrade Backup

Step #	Procedure	Description	
Configu	This procedure is a manual alternative backup. The procedure conducts a full backup of the Configuration database and run environment on site being upgraded, so that each server has the latest data to perform a backout, if necessary.		
number	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step umber.		
1.	Active SOAM CLI: Log into the active SOAM	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active SOAM: ssh admusr@ <soam_vip></soam_vip>	

Step #	Procedure	Description	
2.	Active SOAM CLI: Start a screen session	Enter the command: \$ screen The screen tool creates a no-hang-up shell session, so the command continues to execute if the user session is lost.	
3.	Active SOAM CLI: Execute a backup of all servers managed from the SOAM to be upgraded	Execute the backupAllHosts utility on the active SOAM. This utility remotely accesses each specified server, and runs the backup command for that server. Thesite parameter allows the user to backup all servers associated with a given SOAM site to be upgraded: WARNING: Failure to include thesite parameter with the backupAllHosts command results in overwriting the NOAM backup file created in Section 3.4.4. Backing out to the previous release is not possible if the file is overwritten. \$ /usr/TKLC/dpi/bin/backupAllHostssite= <nename> where <nename> is the Network Element Name (NEName) as seen using the following command: \$ iqt NetworkElement This output displays when executing either of the options: Do you want to remove the old backup files (if exists) from all the servers (y/[n])?y It may take from 10 to 30 minutes for this command to complete, depending upon the number of servers and the data in the database. Do not proceed until the backup on each server is completed. Output similar to the following indicates successful completion: Script Completed. Status: HOSTNAME STATUS HC3blade02 PASS HPC3blade03 PASS HPC3blade04 PASS Errors also report to the command line. Note: There is no progress indication for this command; only the final report when it completes.</nename></nename>	
4.	Active SOAM CLI: Exit the screen session	<pre># exit [screen is terminating] Note: screen -ls is used to show active screen sessions on a server, and</pre>	

Step #	Procedure	Description	
5. □	ALTERNAT IVE METHOD (Optional)	Alternative: A manual back up can be executed on each server individually, rather than using the script. To do this, log into each server in the site individually, and execute the following command to manually generate a full backup on that server:	
	Server CLI:	<pre>\$ sudo /usr/TKLC/appworks/sbin/full_backup</pre>	
	If needed, the	Output similar to the following indicates successful completion:	
	Alternative	Success: Full backup of COMCOL run env has completed.	
	backup method can be executed on each individual server instead of using the backupAIIH osts script	Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullDBParts. SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.	
		Archive file /var/TKLC/db/filemgmt/Backup.dsr.blade01.FullRunEnv. SYSTEM_OAM.20140617_021502.UPG.tar.bz2 written in /var/TKLC/db/filemgmt.	
6.	Active NOAM VIP: Verify backup files are present on each server.	1. Log into the active NOAM GUI using the VIP.	
		2. Navigate to Status & Manage > Files.	
		3. Click on each server tab, in turn.	
		4. For each server, verify the following (2) files have been created:	
		Backup.DSR. <server_name>.FullDBParts.NETWORK_OAMP.<time _stamp>.UPG.tar.bz2</time </server_name>	
		Backup.DSR. <server_name>.FullRunEnv.NETWORK_OAMP.<time_ stamp>.UPG.tar.bz2</time_ </server_name>	
		5. Repeat sub-steps 1 through 4 for each site.	

Appendix F.2. Server Upgrade Using platcfg

The following procedure enables a server to be upgraded using the Platform Configuration (platcfg) utility. This procedure should be used only under the guidance and direction of .

Procedure 49. Server Upgrade Using Platcfg

Step #	Procedure	Description	
This pro	cedure upgrades	a server using the platcfg utility.	
	Note: All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown.		
Check on number		s it is completed. Boxes have been provided for this purpose under each step	
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.	
Log into the server console to be upgraded password:		Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server to be upgraded: ssh admusr@ <server ip=""> password: <enter password=""> Answer yes if you are asked to confirm the identity of the server.</enter></server>	
2.	Server CLI:	Switch to the platcfg user to start the configuration menu.	
	Enter the	\$ sudo su - platcfg	
	platcfg menu	From the Main Menu, select Maintenance	
		Main MenuMaintenanceDiagnosticsServer ConfigurationNetwork ConfigurationRemote ConsolesSecurityNetBackup ConfigurationExitÑ	
3.	Select upgrade	From the Maintenance Menu, select Upgrade. Maintenance Menu Upgrade Backup and Restore Halt Server View Mail Queues Restart Server Eject CDROM Save Platform Debug Logs Exit	

Step #	Procedure	Description
4.	Server CLI: Select early upgrade checks	From the Upgrade Menu, select Early Upgrade Checks. Upgrade Menu Validate Media Early Upgrade Checks Initiate Upgrade Non Tekelec RPM Management Accept Upgrade Reject Upgrade Exit
5.	Server CLI: Select the upgrade media	 6. From the Choose Upgrade Media Menu, select the desired target media. This begins the early upgrade checks in the console window. Choose Upgrade Media Menu Informational messages display as the checks progress. At the end of a successful test, a message similar to this displays: Running earlyUpgradeChecks () for Upgrade::EarlyPolicy:: TPDEarlyChecks upgrade policy Verified server is not pending accept of previous upgrade Hardware architectures match Install products match. Verified server is alarm free! Early Upgrade Checks Have Passed! 7. Verify early upgrade checks pass. In case of errors, it is recommended to contact My Oracle Support (MOS). 8. Press q to exit the screen session and return to the platcfg menu. 9. From the Choose Upgrade Media Menu, select Exit.
6.	Server CLI: Initiate the upgrade	From the Upgrade Menu, select Initiate Upgrade. Upgrade Menu Validate Media Early Upgrade Checks Initiate Upgrade Non Tekelec RPM Management Accept Upgrade Reject Upgrade Exit

Step #	Procedure	Description
7. Server CLI: Select the upgrade media		The screen displays a message that it is searching for upgrade media. Once the upgrade media is found, an Upgrade Media selection menu displayed similar to the example shown. From the Choose Upgrade Media Menu, select the desired target media. This begins the server upgrade. Choose Upgrade Media Menu Choose Upgrade Media Menu Choose Upgrade Media Menu Choose Upgrade Media Menu
		Many informational messages display on the terminal screen as the upgrade proceeds. After upgrade is complete, the server reboots. A reboot of the server is required.
		The server will be rebooted in 10 seconds
8.	Server CLI: Log into the server to be upgraded	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server to be upgraded: ssh admusr@ <server ip=""> password: <enter password=""> Answer yes if you are asked to confirm the identity of the server.</enter></server>
9.	Server CLI: Check for upgrade errors	 Examine the upgrade logs in the /var/TKLC/log/upgrade directory and verify no errors were reported. grep -i error /var/TKLC/log/upgrade/upgrade.log Examine the output of the command to determine if any errors were reported. If the upgrade fails, collect the following files: /var/TKLC/log/upgrade/upgrade.log /var/TKLC/log/upgrade/ugwrap.log /var/TKLC/log/upgrade/earlyChecks.log /var/TKLC/log/platcfg/upgrade.log It is recommended to contact My Oracle Support (MOS) by referring to Appendix U of this document and provide these files.
10.	Server CLI: Verify the upgrade	 Check the upgrade log for the upgrade complete message grep "UPGRADE IS COMPLETE" /var/TKLC/log/upgrade/upgrade.log Verify the UPGRADE IS COMPLETE message displays. If not, it is recommended to contact My Oracle Support (MOS). [admusr@NO2 ~]\$ grep "UPGRADE IS COMPLETE" /var/TKLC/log/ upgrade/upgrade.log 1407786220:: UPGRADE IS COMPLETE

Appendix F.3. Manual DA-MP (N+0) Upgrade Procedure

The following procedure is used to manually upgrade a multi-active DA-MP Server Group. This procedure is provided as an alternative to the normal DA-MP upgrade procedures in Section 5.

Procedure 50 must be executed for all configured DA-MPs of a site, regardless of how the DA-MPs are grouped for upgrade. So if 16 DA-MPs are upgraded four at a time, then Procedure 50 must be executed four distinct times.

Procedure 50. Manual DA-MP (N+0) Upgrade Procedure

Step #	Procedure	Description	
Check o number	This procedure upgrades a multi-active DA-MP servers using the manual upgrade method. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1.	Identify all the DA-MPs to be upgraded together	From the data captured in Table 5, identify the DSR (multi-active cluster) server group to be upgraded.	
2.	Upgrade DA-MP servers as identified in step 1	 Upgrade up to (1/2) one half (no more than 50%) of the DA-MP servers in parallel using the Upgrade Multiple Servers procedure. <i>Note</i>: When using the manual server upgrade method, it is recommended that the DA-MP leader be upgraded in the last group of servers to minimize DA-MP leader role changes. 1. Execute Appendix D Upgrade Multiple Servers – Upgrade Administration. 2. After successfully completing the procedure in Appendix D, return to this point and continue with the next step. 	
3.	Repeat for all servers identified in step 1 of this procedure	Repeat step 2 of this procedure for the remaining DA-MP servers.	

Appendix F.4. ASG SBR Upgrade Procedure

The following procedure is used to upgrade the SBR server group using Auto Server Group upgrade. This procedure is provided as an alternative to the normal SBR upgrade procedures in Section 5.

Procedure 51. ASG SBR Upgrade

Step #	Procedure	Description			
Check o number.	This procedure upgrades the SBR Server Group using the Automated Server Group Upgrade option. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
1.	Identify the SBR server group(s) to upgrade	ended to contact My Oracle Support (MOS) and ask for assistance. From the data captured in Table 5, identify the SBR server group(s) to upgrade. One server group can be executed at a time or multiple server groups can be executed simultaneously.			
2.	Upgrade SBR server group(s) identified in step 1 of this procedure using the upgrade multiple servers procedure	 Note: The spare SBRs of this server group are located at different sites. 1. Use the Automated Server Group Upgrade option. 2. Select the Serial upgrade mode. 3. Execute Appendix D Upgrade Multiple Servers – Upgrade Administration. 			
3.	Repeat for all SBR server groups with active, standby in Site 1 and spare in Site 2 (and an optional 2 nd spare in Site 3)	Repeat step 2 for all remaining binding and session server groups to be upgraded.			

Appendix F.5. Manual SBR Upgrade Procedure

The following procedure is used to upgrade the SBR server group manually. This procedure is provided as an alternative to the normal SBR upgrade procedures in Section 5.

Note: Before upgrading the active SBR, it is imperative that the database audit of the spare and standby servers complete successfully. Failure to comply could result in a loss of session/binding data.

Procedure 52. Manual SBR Upgrade Procedure

Step #	Procedure	Description			
This pro	cedure upgrades ar	n SBR server group using the manual upgrade option.			
	<i>Note</i> : This procedure upgrades all the servers in the server group; however, if it is recommended to upgrade one by one, such as spare, standby, and active in different upgrade iterations. Upgrade those servers manually and then return to this procedure.				
	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
If this pr	If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				

1.		Description		
1.	Active NOAM VIP: Identify the active, standby,		group can be exec	ify the server group(s) to cuted at a time or multiple server
	and spare SBR server group(s)	2. Log into the NOAM G		
	to upgrade	group chosen in sub- spare (as designated	step 1. Note which by the Resource H	Status. Open each server server is active, standby, and IA Role) for each server group e provides an example:
		GTXA-Session1 -	- Active	
		GTXA-Session2 -	- Standby	
		 BarrA-Session-Sl 	^D – Spare	
		BINDING SESSION		
		Server Group Name	Re	source Domain Name
		BarrA_BINDING_SG	BIN	IIDING
		E- GTXA_SESSION_SG	SE	SSION
		Server Name	Resource HA Role	Congestion Level
		BarrA-Session-SP	Spare	Normal
		GTXA-Session1	Active	Normal
		GTXA-Session2	Standby	Normal
		replication of sess replicated configu During this upgra replication of sess the SBR Status s Availability status HA Status screen Upgrade screen r status of the conf Because the two possible that a giv session and bindi	sion or binding data tration data from the de procedure, ONL sion or binding data creen MUST be us (active, standby, contractive, st	lity policies: one for controlling a, and one for receipt of e NOAM and SOAM GUIs. Y the High Availability policy for a is important. This means that ed to determine the High or spare) of SBR servers. The c HA Role column on the because they only show the n policy. Dicies run independently, it is e standby or spare for the ey, but active for the en this happens, it is necessary

Step #	Procedure	Description		
2.	Active NOAM VIP: Upgrade spare SBR server identified in step 1 of this procedure (If need to be upgraded in this upgrade iteration)	 Note: The spare SBRs of this server group are located at different sites. 1. Execute Appendix C Upgrade Single Server – DSR 8.x. 2. After successfully completing the procedure in Appendix C, return to this point to monitor server status. 3. Navigate to SBR > Maintenance > SBR Status. Open the tab of the server group being upgraded. Note: After executing Appendix C, the spare SBR temporarily disappears from the SBR Status screen. When the server comes back online, it reappears on the screen with a status of Out of Service. 4. Monitor the Resource HA Role status of the spare server. Wait for the status to transition from Out of Service to Spare. 5. If the system is equipped with a second spare SBR server, repeat substeps 1 thru 3 for the other spare. Caution: Do not proceed to step 3 until the Resource HA Role of the spare SBR server returns to Spare. 		
3.	Upgrade standby SBR server identified in step 1 of this procedure (If need to be upgraded in this upgrade iteration)	 Execute Appendix C Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and continue with the next step. 		
O	!!WAR	NING!! Failure to comply with step 4 and step 5 may result in the loss of PCA traffic, resulting in service impact.		
4.	Active NOAM VIP: Verify standby SBR server status (If need to be upgraded in this upgrade iteration)	 Navigate to SBR > Maintenance > SBR Status. Open the tab of the server group being upgraded. Note: After executing Appendix C, the standby SBR temporarily disappears from the SBR Status screen, and the spare server assumes the standby role. When the upgraded server comes back online, it reappears on the screen with a status of Out of Service. Monitor the Resource HA Role status of the upgraded server. Wait for the status to transition from Out of Service to Standby. Caution: Do not proceed to step 5 until the Resource HA Role of the upgraded server transitions to Standby. 		

Step #	Procedure	Description		
5.	Active NOAM VIP: Verify bulk download from the active SBR to the standby and spare SBRs completes (If need to be upgraded in this upgrade iteration)	 Navigate to Alarm & Event > View History. Export the Event log using the following filter: Server Group: Choose the SBR group that is in upgrade Display Filter: Event ID = 31127 – DB Replication Audit Complete Collection Interval: X hours ending in current time, where X is the time from upgrade completion of the standby and spare servers to the current time. Wait for all instances of Event 31127: 1 for the Standby binding SBR 1 for the Standby session SBR 1 for the Spare binding SBR 1 for the Spare session SBR 1 for the 3rd site Spare binding SBR (if equipped) 1 for the 3rd site Spare session SBR (if equipped) Note: There is an expected loss of traffic depending on size of the bulk 		
6.	Active SBR (CLI): Verify the replication status for DB Replication and pSbrBindingPoli cy (Binding SBR) Or pSbrSessionPoli cy (Session SBR)	<pre>Alex. This is all objected to be of thing depending on the ortho bank download. This must be noted along with events captured. 1. Use the SSH command (on UNIX systems - or putty if running on windows) to log into the active SBR of the first non-upgraded site: ssh admusr@<sbr_xmi_ip> password: <enter password=""> Answer yes if you are asked to confirm the identity of the server. 2. Execute command irepstat -w Verify replication is showing as Active for ActStb [DbReplication] policy, pSbrSessionPolicy (for Session SBR), and pSbrBindingPolicy (for Binding SBR). Do not proceed if replication is not Active for all of the resource. Example: [admusr@StIhomas-sSBR-A ~]\$ irepstat -w StThomas-sSBR-A C2706.065 stIhomas-sSBR-A 11:19:19 [R] Policy 0 ActStb [DbReplication] BC From D0 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 48.3/s CC To P1 StIhomas-sSBR-B Active 0 0.11 1% 0.08%cpu 48.3/s CC To P1 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 48.3/s CC To P1 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 48.3/s CC To P1 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 48.3/s CC To P1 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 48.3/s CC To P1 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 48.3/s CC To P1 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 62.5/s CC To P1 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 62.5/s CC To P1 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 62.5/s CC To P1 StIhomas-sSBR-B Active 0 0.10 1% 0.08%cpu 62.5/s</enter></sbr_xmi_ip></pre>		

Step #	Procedure	Description
7.	Upgrade active SBR server as identified in step 1 of this procedure (If need to be upgraded in this upgrade iteration)	 Execute Appendix C Upgrade Single Server – DSR 8.x. After successfully completing the procedure in Appendix C, return to this point and continue with the next step.
8.	Repeat for all SBR server groups with active, standby in Site 1 and spare in Site 2	Repeat steps 1 through 6 for all remaining binding and session server groups to be upgraded.

Appendix G. Expired Password Workaround Procedure

This appendix provides the procedures to handle password expiration during upgrade. Procedure 53 is a temporary workaround to allow an expired password to be used on a non-upgrade site. This procedure is provided as a workaround when a password expires after the NOAM has been upgraded and before all sites have been upgraded.

The workaround must be removed using Procedure 54 after the site is upgraded. Failure to remove the workaround inhibits password aging on the server.

Appendix G.1. Inhibit Password Aging

The following procedure enacts a workaround that inhibits password aging on the SOAM. This procedure should be used only when the following conditions apply:

- An upgrade is in progress
- The NOAMs have been upgraded, but one or more sites have not been upgraded
- A login password has expired on a non-upgraded site

Once the workaround is enacted, no passwords expire at that site. Remove the workaround once the site is upgraded.

Procedure 53.	Expired Password Workaround Procedure
---------------	---------------------------------------

Step #	Procedure	De	scription
Check c number	ff ($$) each step as	s it is	vord aging on a server, allowing "expired" credentials to be used for login. completed. Boxes have been provided for this purpose under each step ommended to contact My Oracle Support (MOS) and ask for assistance.
1.	Active SOAM CLI: SSH to active SOAM server. Disable password aging		<pre>windows) to log into the active SOAM of the first non-upgraded site: ssh admusr@<soam_vip> password: <enter password=""> Answer yes if you are asked to confirm the identity of the server. Create a text file with the following content (exactly as formatted): [production] aw.policy.pwchange.isExpired = aw.policy.db.checkPw = [development : production] [test : development]</enter></soam_vip></pre>
		4.	Save the file as: /var/TKLC/appworks/ini/pw.ini Change the file permissions: sudo chmod 644 pw.ini Execute the following command: clearCache
		No	bte : For each server on which this workaround is enacted, the old expired password must be used for login. The new password used on the NOAM does not work on these servers.
2.	Repeat for standby SOAM	Re	peat step 1 for the standby SOAM
3.	Repeat for all non-upgraded sites	Repeat steps 1 and 2 for all non-upgraded sites.	

Appendix G.2. Enable Password Aging

The following procedure removes the password expiration workaround that is enabled by Procedure 53.

Procedure 54. Expired Password Workaround Removal Procedure

Step #	Procedure	Description			
This pro	This procedure removes the password aging workaround and re-enables password aging on a server.				
Check o number.	• • •	it is	completed. Boxes have been provided for this purpose under each step		
If this pr	ocedure fails, it is	reco	mmended to contact My Oracle Support (MOS) and ask for assistance.		
1.	Active SOAM CLI: SSH to active SOAM server. Re- enable	1.	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active SOAM of the first non-upgraded site:		
			ssh admusr@ <soam_vip></soam_vip>		
			password: <enter password=""></enter>		
	password		Answer yes if you are asked to confirm the identity of the server.		
	aging.	2.	Delete the pw.ini file:		
			<pre>\$ sudo rm /var/TKLC/appworks/ini/pw.ini</pre>		
		3.	Execute this command:		
			\$ sudo clearCache		
		4.	Repeat sub-steps 1 through 3 for the standby SOAM		
2. □	Repeat for all non-upgraded sites	Repeat this procedure for all non-upgraded sites.			

Appendix G.3. Password Reset

The following procedure resets the GUI Admin (guiadmin) password on the NOAM. In a backout scenario where the password expired during the upgrade, it is possible for the customer to get locked out due to global provisioning being disabled. When this happens, this procedure can be used to reset the password to gain access to the GUI.

Procedure 55. Expired Password Reset Procedure

Step #	Procedure	De	Description		
This pro	cedure resets the	guia	dmin password on the NOAM.		
number			completed. Boxes have been provided for this purpose under each step mmended to contact My Oracle Support (MOS) and ask for assistance.		
1.	Active NOAM CLI: SSH to	1.	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the active NOAM:		
	active NOAM		ssh admusr@ <noam vip=""></noam>		
	server. Reset the password		password: <enter password=""></enter>		
			Answer yes if you are asked to confirm the identity of the server.		
		2.	Execute the reset command:		
			<pre>\$ sudo /usr/TKLC/appworks/sbin/resetPassword guiadmin</pre>		
		3.	At the Enter new Password for guiadmin prompt, enter a new password.		
		4.	Attempt to log into the NOAM GUI using the new password. If the login is not successful, it is recommended to contact My Oracle Support (MOS) for guidance.		

Appendix H. Network IDIH Compatibility Procedures

The following procedure is used to provide IDIH compatibility when upgrading to Release 8.x. Procedure 56 is performed on a Release 8.x IDIH to make the trace data viewable on prior release IDIH systems, as described in Section 1.7.2. This procedure must be performed on every IDIH 8.x system from which trace data is expected.

When all IDIH systems have been upgraded to Release 8.x, Procedure 57 must be executed on every IDIH on which Procedure 56 was previously performed.

Procedure 56.	Enable IDIH 8.x	Compatibility
---------------	-----------------	---------------

Step #	Procedure	Description			
This pro	This procedure upgrades a server using the platcfg utility.				
	All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown.				
Check c number.		it is completed. Boxes have been provided for this purpose under each step			
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	Appserver Use the SSH command (on UNIX systems – or putty if running on window to log into the appserver:				
	the appserver	ssh admusr@ <server_ip></server_ip>			
		password: <enter password=""></enter>			
		Answer yes if you are asked to confirm the identity of the server.			
2.	Appserver	Change to the system user tekelec:			
	CLI: Change user	sudo su - tekelec			
3.	Appserver	Execute the following command to enable backward compatibility			
	CLI: Execute command	apps/ndih7-compat.sh enable			
4.	Repeat as needed	Repeat this procedure on each IDIH 8.x appserver as needed.			

Procedure 57. Disable IDIH 8.x Compatibility

Step #	Procedure	Description			
This pro	his procedure upgrades a server using the platcfg utility.				
	All UI displays are sample representations of upgrade screens. The actual display may vary slightly for those shown.				
number	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	Appserver CLI: Log into	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the appserver:			
	the appserver	ssh admusr@ <server_ip></server_ip>			
		password: <enter password=""></enter>			
		Answer yes if you are asked to confirm the identity of the server.			

Step #	Procedure	Description
2.	Appserver CLI: Change user	Change to the system user tekelec: sudo su - tekelec
3.	Appserver CLI: Execute command	Execute this command to enable backward compatibility: apps/ndih7-compat.sh disable
4.	Repeat as needed	Repeat this procedure on each IDIH 8.x appserver as needed.

Appendix I. Recover From a Failed Upgrade

The following procedure provides the steps required to recover a server after a failed upgrade. Due to the complexity of the DSR system and the nature of troubleshooting, it is recommended to contact My Oracle Support (MOS) for guidance while executing this procedure.

Design dama 50 Design dama 5 Della della d . . .

Procedure 58. Recover from a Failed Upgrade							
Step #	Procedure	Description					
Note: Check of number.	The server is retur f (√) each step as	ne basic steps for re- rned to the source re it is completed. Bo recommended to co	elease by this xes have bee	procedure. n provided fo	or this purpo	ose unde	r each step
1.	Active NOAM VIP: Select affected server group containing the failed server	 Log into the Ne Navigate to Ac Select the server Main Menu: Administry Filter Tasks T	dministration ver group tab nistration -> S IPFE_SG1 IPFE Upgrade State Server Status Ready Err Failed Err rver was upgr of this proced	 Software for the serve for the serve	r to be reco agement -: PFE_SG4 Server Role Network Elemen System OAM SO1_DSR_VM So1_DSR_VM he Upgrade	> Upgrade MP_s(1) s Function t OAM OAM Server c	Application Ve Upgrade ISO 7.0.1.0.0-70.28 7.0.1.0.0-70.28 DSR-7.2.0.00 option, then

Step #	Procedure	Description			
2.	Active NOAM VIP: Navigate	Navigate to Status & Manage > Tasks > Active Tasks. Connected using INTERNALXMI to NO1 (ACTIVE NETWORK OAM&P)			
	to the Active Tasks screen to view active tasks	 Main Menu Administration Configuration Alarms & Events Security Log Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Active Tasks Scheduled Tasks 			
3.	Active NOAM VIP: Use the filter to locate the server group upgrade task	 From the Filter option, enter the following filter values: Network Element: All Display Filter: Name Like *upgrade* Click Go. Main Menu: Status & Manage -> Tasks -> Active Tasks Filter Filter Filter Filter Reset Display Filter: Name Like *upgrade* Reset R			

Step #	Procedure	Description			
4.	Active NOAM VIP: Identify the upgrade task	 In the search results list, locate the Server Group Upgrade task. 1. If not already selected, select the tab displaying the hostname of the active NOAM server. 2. Locate the task for the Server Group Upgrade. It shows a status of paused. 			
		Filter • NO1 102 SO1 SO2	MP1 MP2 I Status	MP3 MP4 MP6 MP8 Start Time	MP9 MP10 MP11 MP12 Update Time
		SO2 Server Upgrade (m 48 SD_99 Server Group Upgrade)	exception	2016-03-23 13 38 36 070	2016-03-23 13 40 11 6/10
		SO_SG Server Group Upgra	de paused	2016-03-23 13:38:26 UTC	2016-83-23 13:48:07 UTC
		46 SD2 Server Upgrade	exception	2016-03-23 13:14:10 070	2016-03-23 12 16 01 UTC
		44 NO_SG PostUpgrade Healt Check	n completed	2016-03-22 17:14:51 UTC	2016-03-22 17:15:06 UTC
		42 NO_SG PreUpgrade Heath Check	completed	2016-03-21 14:56:08 UTC	2016-03-21 14:55:19 UTC
		upgrade of one exception (i.e., have upgraded still shows as r	e or more ser , failed), while d successfully running. In th	e the other servers y. However, the ser is case, please car	group have status as in that server group rver group upgrade task
		the upgrac server gro	le status of th	ne individual server ve status as compl	p upgrade task, ensure s in that particular eted or exception (that
		Make sure running sta	· · ·	cancelling a task w	ith some servers still in

Step #	Procedure	Description
5.	Active NOAM VIP: Cancel the Server Group Upgrade task	 Click the Server Group Upgrade task to select it. Click Cancel to cancel the task. Click OK on the confirmation screen to confirm the cancellation.
	opgrade task	Main Menu: Status & Manage -> Tasks -> Active Tasks (Filtered)
		Image: Not No2 Sol Sol Sol MP1 MP2 MP3 MP4 MP6 MP8 MP9 MP ID Name Status Start Time Update T
		SO2 Server Upgrade (in 48 SO_SG Server Group exception 2016-03-23 13:38:36 UTC 2016-03- Upgrade)
		47 SO_SG Server Group Upgrade paused 2016-03-23 13:38:26 UTC 2016-03- 46 SO2 Server Upgrade exception 2016-03-23 13:14:10 UTC 2016-03-
		Pause Restart Cancel Delete Report Delete All Completed Delete All Exce
6.	Active NOAM VIP: Verify the Server Group Upgrade task	On the Active Tasks screen, verify the task that was cancelled in step 5 shows a status of completed. 47 SO_SG Server Group Upgride completed 2016-03-23 13:38:26 UTC
	is cancelled	2016-03-23 16:24:27 UTC SG upgrade task cancelled by user. 5%
7.	Failed Server CLI: Inspect upgrade log	Log into the failed server to inspect the upgrade log for the cause of the failure. 1. Use an SSH client to connect to the failed server: ssh <xmi address="" ip=""> login as: admusr</xmi>
		password: <enter password=""> Note: The static XMI IP address for each server should be available in Table 5.</enter>
		 View or edit the upgrade log at /var/TKLC/log/upgrade/upgrade.log for clues to the cause of the upgrade failure.
		 If the upgrade log contains a message similar to the following, inspect the early upgrade log at /var/TKLC/log/upgrade/earlyChecks.log for additional clues.
		1440613685::Early Checks failed for the next upgrade 1440613691::Look at earlyChecks.log for more info

Step #	Procedure	Description
	s s f s s	Ithough outside of the scope of this document, the user is expected to use tandard troubleshooting techniques to clear the alarm condition from the failed erver. troubleshooting assistance is needed, it is recommended to contact My Oracle support (MOS).
8.	Failed Server CLI: Verify platform alarms are cleared from the failed server	Use the alarmMgr utility to verify all platform alarms have been cleared from the system. \$ sudo alarmMgralarmstatus Example output: [admusr@SO2 ~]\$ sudo alarmMgralarmstatus SEQ: 2 UPTIME: 827913 BIRTH: 1458738821 TYPE: SET ALARM: TKSPLATMI10 tpdNTPDaemonNotSynchronizedWarning 1.3.6.1 .4.1.323.5.3.18.3.1.3.10 32509 Communications Communic ations Subsystem Failure ***user troubleshoots alarm and is able to resolve NTP sync issue and clear alarm*** [admusr@SO2 ~]\$ sudo alarmMgralarmstatus [admusr@SO2 ~]\$
9.	Active NOAM VIP: Re- execute the server upgrade	 Return to the upgrade procedure being executed when the failure occurred. Re-execute the upgrade for the failed server using the Upgrade Server option. <i>Note</i>: Once a server has failed while using the Automated Server Group Upgrade option, the Auto Upgrade option cannot be used again on that server group. The remaining servers in that server group must be upgraded using the Upgrade Server option.

Appendix J. Critical and Major Alarms Analysis

The following procedure identifies critical and major alarms that should be resolved before proceeding with an upgrade and backout.

Note: During any time of upgrade if the **31149- DB Late Write Nonactive** alarm displays, ignore it. This alarm does not have any effect on functionality.

Procedure 59. Verify Critical and Major Alarms in the System Before the Upgrade

Step #	Procedure	Description				
This pro	This procedure identifies the current alarms in the system before an upgrade can start.					
Check o number.	· · ·	s it is completed. Boxes have been provided for this purpose under each step				
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	Active NOAM	1. Navigate to Alarms & Events > View Active.				
	VIP : Log/View all	2. Click Report to generate an Alarms report.				
	current alarms at the NOAM	3. Save the report and/or print the report.				
2.	Analyze the	Reference Table 25 and Table 26 for the alarms.				
	active alarms data	If any alarms listed in the Table 25 and Table 26 display in the system, resolve the alarms before starting the upgrade.				
		Refer to Reference [7] DSR Alarms and KPIs Reference for specific alarm in- depth details.				
		Two categories from the alarm list.				
		High impact alarms				
		It's almost certain the presence of this alarm ID in the active alarm list should prevent upgrade from continuing. Alarms of this category should be resolved before upgrading.				
		Medium impact alarms				
		It's likely/possible the presence of this alarm ID should prevent upgrade from continuing; concurrence needed. Alarms of this category may/may not be resolved before upgrading.				
		Some ideas of inclusion of alarms in the categories include.				
		• Any alarm indicating an actual hardware error, or an impending/potential hardware error, is automatically mentioned in high impact alarm list. Included in this category are all Platform Group alarms (PLAT) of severity Minor, Major, and Critical.				
		• If an alarm ID indicates some sort of (pending) resource exhaustion issue or other threshold crossed condition, it is almost always mentioned in Medium impact alarms. Resource exhaustion states have to be fixed before upgrading.				

Table 25.	High	Impact	Alarms
-----------	------	--------	--------

Alarm ID	Name
5010	Unknown Linux iptables command error
5011	System or platform error prohibiting operation

Alarm ID	Name
10000	Incompatible database version
10134	Server Upgrade Failed
10200	Remote database initialization in progress
19217	Node isolated - all links down
19805	Communication Agent Failed to Align Connection
19855	Communication Agent Resource Has Multiple Actives
19901	CFG-DB Validation Error
19902	CFG-DB Update Failure
19903	CFG-DB post-update Error
19904	CFG-DB post-update Failure
22223	MpMemCongested
22950	Connection Status Inconsistency Exists
22961	Insufficient Memory for Feature Set
22733	SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration
22734	Policy and Charging Unexpected Stack Event Version
25500	No DA-MP Leader Detected
25510	Multiple DA-MP Leader Detected
31101	Database replication to slave failure
31116	Excessive shared memory
31117	Low disk free
31125	Database durability degraded
31128	ADIC Found Error
31133	DB Replication Switchover Exceeds Threshold
31215	Process resources exceeded
31288	HA Site Configuration Error
32100	Breaker Panel Feed Unavailable
32101	Breaker Panel Breaker Failure
32102	Breaker Panel Monitoring Failure
32103	Power Feed Unavailable
32104	Power Supply 1 Failure
32105	Power Supply 2 Failure
32106	Power Supply 3 Failure
32107	Raid Feed Unavailable
32108	Raid Power 1 Failure
32109	Raid Power 2 Failure

Alarm ID	Name
32110	Raid Power 3 Failure
32111	Device Failure
32112	Device Interface Failure
32113	Uncorrectable ECC memory error
32114	SNMP get failure
32115	TPD NTP Daemon Not Synchronized Failure
32116	TPD Server's Time Has Gone Backwards
32117	TPD NTP Offset Check Failure
32300	Server fan failure
32301	Server internal disk error
32302	Server RAID disk error
32303	Server Platform error
32304	Server file system error
32305	Server Platform process error
32306	Server RAM shortage error
32307	Server swap space shortage failure
32308	Server provisioning network error
32309	Eagle Network A Error
32310	Eagle Network B Error
32311	Sync Network Error
32312	Server disk space shortage error
32313	Server default route network error
32314	Server temperature error
32315	Server mainboard voltage error
32316	Server power feed error
32317	Server disk health test error
32318	Server disk unavailable error
32319	Device error
32320	Device interface error
32321	Correctable ECC memory error
32322	Power Supply A error
32323	Power Supply B error
32324	Breaker panel feed error
32325	Breaker panel breaker error
32326	Breaker panel monitoring error

Alarm ID	Name
32327	Server HA Keep alive error
32328	DRBD is unavailable
32329	DRBD is not replicating
32330	DRBD peer problem
32331	HP disk problem
32332	HP Smart Array controller problem
32333	HP hpacucliStatus utility problem
32334	Multipath device access link problem
32335	Switch link down error
32336	Half Open Socket Limit
32337	Flash Program Failure
32338	Serial Mezzanine Unseated
32339	TPD Max Number Of Running Processes Error
32340	TPD NTP Daemon Not Synchronized Error
32341	TPD NTP Daemon Not Synchronized Error
32342	NTP Offset Check Error
32343	TPD RAID disk
32344	TPD RAID controller problem
32345	Server Upgrade snapshot(s) invalid
32346	OEM hardware management service reports an error
32347	The hwmgmtcliStatus daemon needs intervention
32348	FIPS subsystem problem
32349	File Tampering
32350	Security Process Terminated
32500	Server disk space shortage warning
32501	Server application process error
32502	Server hardware configuration error
32503	Server RAM shortage warning
32504	Software Configuration Error
32505	Server swap space shortage warning
32506	Server default router not defined
32507	Server temperature warning
32508	Server core file detected
32509	Server NTP Daemon not synchronized
32510	CMOS battery voltage low

Alarm ID	Name	
32511	Server disk self-test warning	
32512	Device warning	
32513	Device interface warning	
32514	Server reboot watchdog initiated	
32515	Server HA failover inhibited	
32516	Server HA Active to Standby transition	
32517	Server HA Standby to Active transition	
32518	Platform Health Check failure	
32519	NTP Offset Check failure	
32520	NTP Stratum Check failure	
32521	SAS Presence Sensor Missing	
32522	SAS Drive Missing	
32523	DRBD failover busy	
32524	HP disk resync	
32525	Telco Fan Warning	
32526	Telco Temperature Warning	
32527	Telco Power Supply Warning	
32528	Invalid BIOS value	
32529	Server Kernel Dump File Detected	
32530	TPD Upgrade Failed	
32531	Half Open Socket Warning Limit	
32532	Server Upgrade Pending Accept/Reject	
32533	TPD Max Number Of Running Processes Warning	
32534	TPD NTP Source Is Bad Warning	
32535	TPD RAID disk resync	
32536	TPD Server Upgrade snapshot(s) warning	
32537	FIPS subsystem warning event	
32538	Platform Data Collection Error	
32539	Server Patch Pending Accept/Reject	
32540	CPU Power limit mismatch	

Table 26. Medium Impact Alarms

Alarm ID	Name	
5002	IPFE Address configuration error	
5003	IPFE state sync run error	

Alarm ID	Name	
5004	IPFE IP tables configuration error	
5006	Error reading from Ethernet device	
5012	Signaling interface heartbeat timeout	
5013	Throttling traffic	
5100	Traffic overload	
5101	CPU Overload	
5102	Disk Becoming Full	
5103	Memory Overload	
10003	Database backup failed	
10006	Database restoration failed	
10020	Backup failure	
10117	Health Check Failed	
10118	Health Check Not Run	
10121	Server Group Upgrade Cancelled - Validation Failed	
10123	Server Group Upgrade Failed	
10131	Server Upgrade Cancelled (Validation Failed)	
10133	Server Upgrade Failed	
10141	Site Upgrade Cancelled (Validation Failed)	
10143	Site Upgrade Failed	
19200	RSP/Destination unavailable	
19202	Linkset unavailable	
19204	Preferred route unavailable	
19246	Local SCCP subsystem prohibited	
19251	Ingress message rate	
19252	PDU buffer pool utilization	
19253	SCCP stack event queue utilization	
19254	M3RL stack event queue utilization	
19255	M3RL network management event queue utilization	
19256	M3UA stack event queue utilization	
19258	SCTP Aggregate Egress queue utilization	
19251	Ingress message rate	
19252	PDU buffer pool utilization	
19253	SCCP stack event queue utilization	
19254	M3RL stack event queue utilization	
19255	M3RL network management event queue utilization	

Alarm ID	Name	
19256	M3UA stack event queue utilization	
19258	SCTP Aggregate Egress queue utilization	
19272	TCAP active dialogue utilization	
19273	TCAP active operation utilization	
19274	TCAP stack event queue utilization	
19276	SCCP Egress Message Rate	
19408	Single Transport Egress-Queue Utilization	
19800	Communication Agent Connection Down	
19803	Communication Agent stack event queue utilization	
19806	Communication Agent CommMessage mempool utilization	
19807	Communication Agent User Data FIFO Queue Utilization	
19808	Communication Agent Connection FIFO Queue utilization	
19818	Communication Agent DataEvent Mempool utilization	
19820	Communication Agent Routed Service Unavailable	
19824	Communication Agent Pending Transaction Utilization	
19825	Communication Agent Transaction Failure Rate	
19827	SMS stack event queue utilization	
19846	Communication Agent Resource Degraded	
19847	Communication Agent Resource Unavailable	
19848	Communication Agent Resource Error	
19860	Communication Agent Configuration Daemon Table Monitoring Failure	
19861	Communication Agent Configuration Daemon Script Failure	
19862	Communication Agent Ingress Stack Event Rate	
19900	Process CPU Utilization	
19905	Measurement Initialization Failure	
19910	Message Discarded at Test Connection	
8000-001	MpEvFsmException_SocketFailure	
8000-002	MpEvFsmException_BindFailure	
8000-003	MpEvFsmException_OptionFailure	
8000-101	MpEvFsmException_ListenFailure	
8002-003	MpEvRxException_CpuCongested	
8002-004	04 MpEvRxException_SigEvPoolCongested	
8002-006	MpEvRxException_DstMpCongested	
8002-007	MpEvRxException_DrlReqQueueCongested	
8002-008	MpEvRxException_DrlAnsQueueCongested	

Alarm ID	Name	
8002-009	MpEvRxException_ComAgentCongested	
8002-203	MpEvRxException_RadiusMsgPoolCongested	
8006-101	EvFsmException_SocketFailure	
8011	EcRate	
8013	MpNgnPsStateMismatch	
8200	MpRadiusMsgPoolCongested	
8201	RclRxTaskQueueCongested	
8202	RclltrPoolCongested	
8203	RcITxTaskQueueCongested	
8204	RclEtrPoolCongested	
22016	Peer Node Alarm Aggregation Threshold	
22017	Route List Alarm Aggregation Threshold	
22056	Connection Admin State Inconsistency Exists	
22200	MpCpuCongested	
22201	MpRxAllRate	
22202	MpDiamMsgPoolCongested	
22203	PTR Buffer Pool Utilization	
22204	Request Message Queue Utilization	
22205	Answer Message Queue Utilization	
22206	Reroute Queue Utilization	
22207	DclTxTaskQueueCongested	
22208	DclTxConnQueueCongested	
22214	Message Copy Queue Utilization	
22221	Routing MPS Rate	
22222	Long Timeout PTR Buffer Pool Utilization	
22349	IPFE Conneetion Alarm Aggregation Threshold	
22350	Fixed Connection Alarm Aggregation Threshold	
22407	Routing attempt failed duto internal database inconsistency failure	
22500	DSR Application Unavailable	
22501	DSR Application Degraded	
22502	DSR Application Request Message Queue Utilization	
22503	DSR Application Answer Message Queue Utilization	
22504	DSR Application Ingress Message Rate	
22607	Routing attempt failed due to DRL queue exhaustion	
22608	Database query could not be sent due to DB congestion	

Alarm ID	Name		
22609	Database connection exhausted		
22631	FABR DP Response Task Message Queue Utilization		
22632	COM Agent Registration Failure		
22703	Diameter Message Routing Failure Due to Full DRL Queue		
22710	SBR Sessions Threshold Exceeded		
22711	SBR Database Error		
22712	SBR Communication Error		
22717	SBR Alternate Key Creation Failure Rate		
22720	Policy SBR To PCA Response Queue Utilization Threshold Exceeded		
22721	Policy and Charging Server In Congestion		
22722	Policy Binding Sub-resource Unavailable		
22723	Policy and Charging Session Sub-resource Unavailable		
22724	SBR Memory Utilization Threshold Exceeded		
22725	SBR Server In Congestion		
22726	SBR Queue Utilization Threshold Exceeded		
22727	SBR Initialization Failure		
22728	SBR Bindings Threshold Exceeded		
22729	PCRF Not Configured		
22730	Policy and Charging Configuration Error		
22731	Policy and Charging Database Inconsistency		
22732	SBR Process CPU Utilization Threshold Exceeded		
22737	Configuration Database Not Synced		
22740	SBR Reconfiguration Plan Completion Failure		
31100	Database replication fault		
31102	Database replication from master failure		
31103	DB Replication update fault		
31104	DB Replication latency over threshold		
31106	Database merge to parent failure		
31107	Database merge from child failure		
31108	Database merge latency over threshold		
31113	DB replication manually disabled		
31114	DB replication over SOAP has failed		
31118	Database disk store fault		
31121	Low disk free early warning		
31122	Excessive shared memory early warning		

Alarm ID	Name		
31124	ADIC error		
31126	Audit blocked		
31130	Network health warning		
31131	DB Ousted Throttle Behind		
31134	DB Site Replication To Slave Failure		
31135	DB Site Replication to Master Failure		
31137	DB Site Replication Latency Over Threshold		
31146	DB mastership fault		
31147	DB upsynclog overrun		
31200	Process management fault		
31201	Process not running		
31202	Unkillable zombie process		
31209	Hostname lookup failed		
31217	Network Health Warning		
31220	HA configuration monitor fault		
31113	DB replication manually disabled		
31114	DB replication over SOAP has failed		
31118	Database disk store fault		
31121	Low disk free early warning		
31122	Excessive shared memory early warning		
31124	ADIC error		
31126	Audit blocked		
31130	Network health warning		
31131	DB Ousted Throttle Behind		
31134	DB Site Replication To Slave Failure		
31135	DB Site Replication to Master Failure		
31137	DB Site Replication Latency Over Threshold		
31146	DB mastership fault		
31147	DB upsynclog overrun		
31200	Process management fault		
31201	Process not running		
31202	Unkillable zombie process		
31209	Hostname lookup failed		
31217	Network Health Warning		
31220	HA configuration monitor fault		

Alarm ID	Name	
31221	HA alarm monitor fault	
31222	HA not configured	
31233	HA Heartbeat transmit failure	
31224	HA configuration error	
31225	HA service start failure	
31226	HA availability status degraded	
31228	HA standby offline	
31230	Recent alarm processing fault	
31231	Platform alarm agent fault	
31233	HA Path Down	
31234	Untrusted Time Upon Initialization	
31234	Untrusted time After Initialization	
31236	HA Link Down	
31282	HA Management Fault	
31283	Lost Communication with server	
31322	HA Configuration Error	
33001	Diameter-to-MAP Service Registration Failure on DA-MP	
33105	Routing Attempt failed due to queue exhaustion	
33120	Policy SBR Binding Sub-Resource Unavailable	
33301	Update Config Data Failure	
33303	U-SBR Event Queue Utilization	
33310	U-SBR Sub-resource Unavailable	
33312	DCA Script Generation Error	
33301	Update Config Data Failure	

Appendix K. Additional Backout Steps

Procedure 60. Additional Backout Steps for NOAM, SOAM, and SBR Server(s)

Step #	Procedure	Description	
to suppo Check o	This procedure provides the details about additional backout steps for NOAM, SOAM and SBR server(s) to support backout for major upgrade release paths. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.		
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.	
1.	Server CLI: Log into the server (if not already done)	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server under backout: ssh admusr@ <server address=""> password: <enter password=""> Answer yes if you are asked to confirm the identity of the server. If server is NOAM or SOAM server, execute steps 2 to 5 and if server is SBR server, execute steps 6. to 7. Please note down the hostname of the server on which these steps are executed. Once all the servers in a server group will be backed out then the additional post-backout steps will be executed to revert back the changes done in this procedure.</enter></server>	
2.	Server CLI: Set the resource as optional For OAM servers only	 Note: Make sure the resource being set is in system. Some of the resources shown are introduced in different releases. If the resource is not in the system, presence check will not result any output records. In this case, skip updating these fields for the resource not in the system. 1. Check for the resource: iqt -E HaResourceCfg where "name='<resource_name>'"</resource_name> 2. Execute this command: iset -W -foptional='Yes' HaResourceCfg where "name='DSROAM_Proc'" These commands change/update the results of some records. 	
3.	Server CLI: Restart the HTTPD service For OAM servers only	Execute this command: sudo service httpd restart	
4.	Active NOAM/SOAM Server CLI: Log into the server (if not already done)	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the Active NOAM/SOAM server in the same server group, in which server is under backout: ssh admusr@ <server address=""> password: <enter password=""> Answer yes if you are asked to confirm the identity of the server.</enter></server>	

Step #	Procedure	Description
5.	Server CLI: Verify that the	 Execute this command on an active NOAM/SOAM server in the same server group being backed out:
	replication is working fine.	irepstat
	For OAM servers only	2. Verify the <i>irepstat</i> command displays a replication row for the server which is being backed out.
		Note the replication status is Active before proceeding, if it is Audit , then wait until replication becomes Active.
		If this step is missed, data is lost and is unrecoverable.
		Example:
		Here Ford-B-NO is Active NOAM Server and Ford-A-NO is backed out.
		Ford-B-NO A3301.157 Ford-B-NO 09:32:17 [Rw]
		Policy 0 ActStb [DbReplication]
		AA To P0 Ford-A-NO Active 0 0.000 1%R 0.12%cpu 1.88k/s AA To P1 Chevy-DRNO-B Active 0 0.000 1%R 0.08%cpu 1.89k/s
		AA To P1 Chevy-DRNO-B Active 0 0.00 1%R 0.08%cpu 1.89k/s AB To D0 Camaro-SO-B Active 0 0.00 1%R 0.09%cpu 1.89k/s
		AB To DO Nova-SO-B Active 0 0.00 1%R 0.08%cpu 1.90k/s
		AB TO DO Pinto-SO-B Active 0 0.00 1%R 0.10%cpu 1.89k/s
		AB TO DO Mustang-SO-B Active 0 0.00 1%R 0.10%cpu 2.14k/s
		3. Press q if you want to exit the irepstat command output.
		4. Execute irepstat again, if required.
6.	Server CLI: Setting the resource as optional For SBR servers only	Note: Make sure the resource being set is in the system. Some of the resources listed below are introduced in different releases.
		If a resource is not in the system, presence check does not result in any output records. In this case, do not update the fields for the resource.
		Resource presence can be checked using:-
		iqt -E HaResourceCfg where "name=' <resource_name>'"</resource_name>
		For example:-
		iqt -E HaClusterResourceCfg where "resource='uSbrRes'"
		Execute this command for Session SBR only:
		iset -W -foptional='Yes' HaResourceCfg where "name='pSbrSBaseRepl'"
		iset -W -foptional='Yes' HaClusterResourceCfg where "resource='uSbrRes'"
		iset -W -foptional='Yes' HaClusterResourceCfg where "resource='pSbrSessionRes'"
		Execute this command for Binding SBR only:
		iset -W -foptional='Yes' HaResourceCfg where "name='pSbrBBaseRepl'"
		iset -W -foptional='Yes' HaClusterResourceCfg where "resource='uSbrRes'"
		iset -W -foptional='Yes' HaResourceCfg where "name='pSbrBindingRes'"
		These commands change/update the results of some records.

Step #	Procedure	Description
7.	Server CLI: Verify that the replication is working fine For SBR servers only	 Execute this command on an active SBR server in the same server group as the server being backed out: irepstat Verify the irepstat command displays a replication row for the server which is being backed out. Note the replication status is Active before proceeding, if it is Audit, then wait until replication becomes Active. If this step is missed, data is lost and is unrecoverable. Example: Here Pinto-SBR-2 is Active SBR Server and Pinto-SBR-1 is backed out. Also, on Binding SBR, resource will be pSbrBindingPolicy And on Session SBR, resource will be pSbrSessionPolicy Pinto-SBR-2 C3783.034 Pinto-SBR-2 13:39:38 [Rw] Policy 0 ActStb [DbReplication]

Appendix L. Additional Post-Backout Steps

Procedure 61. Additional Post Backout Steps for NOAM, SOAM, and SBR Server(s)

Step #	Procedure	Description			
	This procedure provides the details about additional post backout steps for NOAM, SOAM and SBR server(s) to support backout for major upgrade release paths.				
This pro	cedure is execute	ed only after all servers in the same server group are backed out.			
Check o number.	• •	s it is completed. Boxes have been provided for this purpose under each step			
If this pr	ocedure fails, it is	s recommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	Server CLI: Log into the server (if not already done)	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server under backout: ssh admusr@ <server address=""> password: <enter password=""> Answer yes if you are asked to confirm the identity of the server. If the server is an NOAM or SOAM server, execute step 2. If the server is an SBR server, execute steps 3. Note the hostname of the server on which these steps are executed. Once all servers in a server group are backed out, additional post-backout steps are executed to revert the changes done in this procedure. Execute the following commands on servers where the services are in pending state: rm -rf /etc/ld.so.cache echo "/usr/TKLC/dsr/lib" sudo tee -a /etc/ld.so.conf.d/dsr.conf sudo cat /etc/ld.so.conf.d/dsr.conf sudo ldconfig Check for configured libraries, for example: sudo ldconfig -p grep -i pdra Output must have the following information: libPdraTraps.so (libc6,x86-64) => /usr/TKLC/dsr/lib/libPdraTraps.so Check whether all the services are Up:</enter></server>			
2.	Server CLI:	pl Note: Make sure the resource getting set is in system. Some of resources			
	Set the resource as optional For OAM servers only	 shown are introduced in different releases. If the resource is not in the system, presence check will not result any output records. In this case, skip updating these fields for the resource not in the system. 1. Check for the resource: iqt -E HaResourceCfg where "name='<resource_name>'"</resource_name> 2. Execute this command: iset -W -foptional='Yes' HaResourceCfg where "name='DSROAM_Proc'" These commands change/update the results of some records. 			

Step #	Procedure	Description
3. □	Server CLI: Setting the	Note: Make sure the resource being set is in the system. Some of the resources listed below are introduced in different releases.
	resource as optional For SBR	If a resource is not in the system, presence check does not result in any output records. In this case, do not update the fields for the resource.
	servers only	Resource presence can be checked using:-
	-	iqt -E HaResourceCfg where "name=' <resource_name>'"</resource_name>
		For example:-
		iqt -E HaClusterResourceCfg where "resource='uSbrRes'"
		Execute this command for Session SBR only:
		iset -W -foptional='No' HaResourceCfg where "name='pSbrSBaseRepl'"
		<pre>iset -W -foptional='No' HaClusterResourceCfg where "resource='uSbrRes'"</pre>
		iset -W -foptional='No' HaClusterResourceCfg where "resource='pSbrSessionRes'"
		Execute this command for Binding SBR only:
		iset -W -foptional='No' HaResourceCfg where "name='pSbrBBaseRepl'"
		iset -W -foptional='No' HaClusterResourceCfg where "resource='uSbrRes'"
		iset -W -foptional='No' HaResourceCfg where "name='pSbrBindingRes'"
		These commands change/update the results of some records.
		Repeat this procedure for other servers in the server group being backed out.

Appendix M.Manual Completion of Server Upgrade

Procedure 62. Manual Completion of Server Upgrade

Step #	Procedure	Description				
This pro	This procedure provides the details about manual completion of server upgrade.					
	and the Status M upgrade, then pe	rent that after the upgrade, if the Upgrade State of server is Backout Ready Message displays Server could not restart the application to complete the erform to restore the server to full operational status and return to this step to rade. Perform Appendix U to create a link of Comagent				
Check of number.		s it is completed. Boxes have been provided for this purpose under each step				
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.				
1. □	NOAMP VIP GUI: Login: Log into the	If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server.				
	server (if not	Open the web browser and enter a URL of:				
	already done)	http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>				
		Log into the NOAM GUI as the guiadmin user:				
		ORACLE				
		Oracle System Login Tue Jun 7 13:49:06 2016 EDT				
		Log In Enter your username and password to log in Username: Password: Change password Log In				
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.				
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, <u>Oracle</u> and/or its affiliates. All rights reserved.				

Step #	Procedure	Description					
2. □	NOAMP VIP GUI: Verify	1. Navigate to Sta	itus and Man	age > HA	۸.		
	server status	2. Locate the serv	er you want te	o upgrade	Э.		
		3. Verify the Max		ole is Sta	ndby.		
		Filter* •					
		Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List	Network Element
		Ford-4-ND	Standby	NA	Active	Ford-B-NO	NO_Ford
		Ford-B-NO	Active	N/A	Active	Ford-A-NO	NO_Ford
		Mustang-MP1	Active	Active	Active	Mustang-MP2	SO_Mustang
		Mustang-MP2	Standby	Active	Standby	Mustang-MP1	SO_Mustang
		Pirito-NP1	Standby	Active	Active	Finto-MP2	SO_Pinto
		Pinto-MP2	Active	Active	Active	Pinto-MP1	SO_Pinto
		Mustang-SO-8p	Spare	NA	Active	Pinto-SO-A Pinto-SO-E	SO_Mustang
		Pinto-SO-Sp	Spare	N/A	Active	Mustang-SO-A Mustang-SO-B	SO_Pinto
		Mustang-SBR-1	Active	Active	Active	Mustang-SBR-2 Finto-SBR-3	SO_Mustang
		Mustang-SBR-2	Standby	Standby	Active	Mustang-SBR-1 Pinto-SBR-3	SO_Mustang
		Mustang-SBR-3	Spare	Spare	Active	Pinto-SBR-1 Pinto-SBR-2	SO_Mustang
		Pinto-SBR-1	Standby	Standby	Active	Mustang-SBR-3 Pinto-SBR-2	SO_Pinto
		Pinto-SBR-2	Active	Active	Active	Mustang-SBR-3 Pinto-SBR-1	SO_Pinto
		Plinto-SBR-3	Spare	Spare	Active	Mustang-SBR-1 Mustang-SBR-2	SO_Pinto
		Edit 4. Click Edit.				Real (44, 80 B)	

Step #	Procedure	Description					
3.	NOAMP VIP GUI: Change role	 Change the Max Allowed HA Role to Active. Click OK. Main Menu: Status & Manage -> HA [Edit] 					
		Modifying H	IA attributes				
		Hostname	Max Allowed HA Role	e Description			
		Ford-A-NO	Active	The maximum	n desired HA	Role for Ford-A-NO	
		Ford-B-NO	Active 💌	The maximum	n desired HA	Role for Ford-B-NO	
		Mustang-MP1	Active 💌	The maximun	n desired HA	Role for Mustang-Mi	P1
		Mustang-MP2	Active	The maximur	n desired HA	Nole for Mustang-Mi	P2
		Pinto-MP1	Active 💌	The maximur	n desired HA	Role for Pinto-MP1	
4.	NOAMP VIP GUI: Verify change	9335 A	x Allowed HA F tus & Manage -> HA	tole change	es to Act	ive.	
	change	Filter* *					
		Hostname	OAM HA R	ole Application HA	Max Allowed HA Role	Mate Hostname List	Network Element
		Ford-A-NO	Standby	N/A	Active	Ford-B-NO	NO_Ford
		Ford-B-NO	Active	NIA	Active	Ford-A-NO	NO_Ford
		Mustang-MP1	Active	Active	Active	Mustang-MP2	SO_Mustang
		Mustang-MP2	Standby	Active	(Active)	Mustang-NP1	SO_Mustang
		Pinto-MP1	Standby	Active	Active	Pinto-MP2	SO_Pinto
		Panto-MP2	Adive	Active	Active	Pinto-MP1	SO_Pinto
		Mustang-90-Sp	Spare	NUA	Active	Pinto-SO-A Pinto-SO-B	SO_Mustang

Step #	Procedure	Description					
5. □	NOAMP VIP GUI: Restart the server	 Navigate to Status & Manage > Server. Select the server to upgrade. 					
		3. Click Restart .					
		Main Menu: Status & Manage	-> Server				
		Filter* *					
		Server Hostname	Network Element	Annel State			
		Second		Appl State			
		Ford-A-ND	NO_Ford	Enabled			
		Ford-B-NO	NO_Ford	Enabled			
		Mustang-MP1		Enabled			
		Mustang-MP2	SO_Mustang	Contraction of the second seco			
		Mustang-SBR-1	SO_Mustang	Enabled			
		Mustang-SBR-2 Mustang-SBR-3	SO_Mustang	Enabled			
		Mustang-SBR-3 Mustang-SBR-4	SO_Mustang SO_Mustang	Enabled			
		Mustang-SBR-5	SO_Mustang	Enabled			
		Mustang-SBR-6	SO_Mustang	Enabled			
		Mustang-SO-A	SO_Mustang	Enabled			
		Mustang-SO-B	SO_Mustang	Enabled			
		Mustang-SO-Sp	SO_Mustang	Enabled			
		Nova-MP1	SO_Nova	Enabled			
		Nova-MP2	SO_Nova	Enabled			
		Nova-SER-1	3D_Nova	Enabled			
		Nova-SBR-2	SO_Nova	Enabled			
		Nova-SBR-3	SO_Nova	Enabled			
		Nova-SBR-4	SO_Nova	Enabled			
		Nora,980,6	90 Nasa	Enshied			
			e Appl State change to Ena				
6.	NOAMP VIP GUI: Verify status	2. Verify the Upgrade Sta Message changes to \$ Main Menu: Administration → Software Man (Here > 1995 → Precipion Chec. (1001 10) Carters. (10, 10) Manual State Constant Manual State Constate Constant Manual State	All St. St. Henr, 20, 20. Parts, 20, 20. Starter Rate Factore Application Version Server Rate Sources Server Starter Server Starter Server Server Starter Server Starter Server Starte	eject and the Status			
		Marting 4072	009452005,8243-65,54 009452005,8243-65,54 009452005,8243-65,54	us Coorer Dener oppinde to template			
		Accept at Report Adve	MP polve 8.20.0.8-82.5.0 (haller)	2017-16-25 06.99.37 EDF 2017-16-28 98 84 88 EDF			

Appendix N. Identify the DC server

Procedure 63. Identification of the DC server

Step #	Procedure	Description				
Check o number	ff ($√$) each step as	e details to identify the DC server. it is completed. Boxes have been provided for this purpose under each step				
If this pr	ocedure fails, it is r	s recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.		Open the web browser and enter a URL of:				
	GUI: Login	http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>				
		Log into the NOAM GUI as the guiadmin user:				
		ORACLE [®] Oracle System Login				
		Tue Jun 7 13:49:06 2016 EDT				
		Log In Enter your username and password to log in Username: Password: Change password Log In				
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.				
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, <u>Oracle</u> and/or its affiliates. All rights reserved.				
2.	NOAMP VIP GUI: Select an MP server	 Navigate to Configuration > Server Groups. Select an MP server from the server group that needs to be upgraded. 				
3.	Log into MP Server using CLI SSH to MP server chosen above	 Use the SSH command (on UNIX systems – or putty if running on windows) to log into the MP server identified in Step 1. ssh admusr@<mp_server_xmi></mp_server_xmi> password: <enter password=""></enter> Answer yes if you are asked to confirm the identity of the server 				

Step #	Procedure	Description
Step #	Procedure MP Server CLI: Find DC server	Description Identify the DC server in the server group with this command: ha.info -d If the server is the DC server, then output is similar to this: [admusr@X6201-MP1 ~]\$ ha.info -d Output from Node ID: X6201-MP1 Report Time: 12/14/2017 12:05:10.905 *** ** Election Mgr: C2121 (27a64d) *** DC: X6201-MP1 Generation: 2 State: DC Elected: 12/12/2017 09:18:08.905
		Other Non-DC Group Members: X6201-MP5 X6201-MP3 X6201-MP4 X6201-MP2 DC Group Candidates: <none> *** ** End of Election Mgr: C2121</none>
		<pre>*** If the server is not the DC server, then output is similar to this: [admusr@X6201-MP3 ~]\$ ha.info -d Output from Node ID: X6201-MP3 Report Time: 12/14/2017 12:05:38.314 *** *** Election Mgr: C2121 (27a64d) *** DC: X6201-MP1 Generation: 2 State: NON-DC</pre>
		<pre>DC: X6201-MP1 Generation: 2 State: NON-DC ATTN: Reported from Non-DC node. Execute ha.info on DC for full status. DC Group Candidates: <none> *** *** End of Election Mgr: C2121 ***</none></pre>

Appendix O. Limitations of Automated Server Group and Automated Site Upgrade

For multi-active server groups, such as DA-MP/vSTP MPs, non-deterministic server selection **could possibly** result in a network outage during the upgrade. In certain scenarios, customer preferences or requirements can result in configurations in which it is imperative that DA-MP servers must be, or conversely, cannot be, upgraded together. These scenarios are described in this section with the recommendation that customers NOT use ASG if any of these exists in their network.



Specialized Fixed Diameter Connections

In this scenario, each peer node is configured to connect to two specific DA-MPs for local redundancy (Figure 18). With ASG/ASU setup for 50% minimum availability, three of the DA-MPs in the server group are upgraded in parallel. However, it is not possible to determine in advance which three DA-MPs are selected. Although the DSR has redundant connections to the peer nodes, an unfortunate selection of servers for upgrade could result in an outage. Upgrade cycle 1 takes out both DA-MPs connected to the unhappy peer. This peer is isolated for the duration of the upgrade.

The happy peer is connected to DA-MPs that are selected by ASG/ASU for different upgrade cycles. This peer is never isolated during the upgrade.

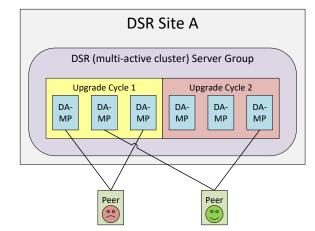


Figure 18. Specialized Fixed Diameter Connections

Specialized Floating Diameter Connections

In this scenario, each peer node is configured to connect to an IPFE TSA address hosted by a set of DA-MPs. When any particular TSA contains only a subset of the server group MPs, and the DSR upgrade logic happens to select that subset of MPs for simultaneous upgrade, then there is a signaling outage for that TSA. This scenario is depicted in Figure 19.

TSA1 is distributed across the first three DA-MPs, whereas TSA2 is distributed across all six DA-MPs. If ASG/ASU is initiated with 50% minimum availability, the DSR could select all three of the DA-MPs hosting TSA1 in the first upgrade cycle. The unhappy peer is isolated for the duration of upgrade cycle 1.

The happy peer is connected to TSA2, which is hosted by the DA-MP servers in such a way that the TSA is evenly hosted in both upgrade cycles. This peer is never isolated during the upgrade.

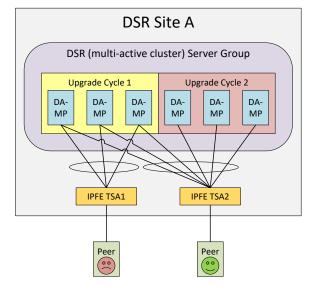
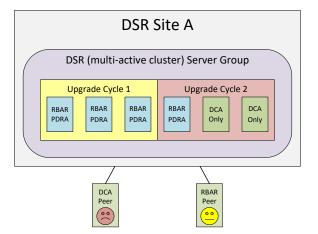


Figure 19. Specialized Floating Diameter Connections

Specialized Distribution of DSR Features

In this scenario, the customer has decided to enable P-DRA and RBAR on four DA-MP servers and DCA on two DA-MP servers, consistent with expected traffic load. With ASG setup for 50% minimum availability, the DA-MP server group is upgraded in two cycles. RBAR and P-DRA happen to be hosted by DA-MP servers selected by ASG/ASU to be in different upgrade cycles, albeit unbalanced. The RBAR peer is only marginally happy because during upgrade cycle 1, only 25% of RBAR and P-DRA capacity is available, even though the customer specified 50% availability.

DCA happens to be hosted by DA-MP servers selected by ASG/ASU to be in upgrade cycle 2. The DCA peer is unhappy because DCA is completely unavailable during upgrade cycle 2.





Appendix P. Advanced Health Check Procedure

Procedure 64. Firewall Check for DNS Port 53

Step #	Procedure	Description
	AM and each SC	he UDP/TCP port 53 is open between NOAM and each DR-NOAM DAM site, and between MPs and each name server of the file
	ff ($$) each step a prime	as it is completed. Boxes have been provided for this purpose under
If this praises assistan		s recommended to contact My Oracle Support (MOS) and ask for
1.	Verify if the	From the command prompt of the server with the alarm:
	UDP/TCP port 53 is	 Issue the sudo nmap -sTU -p 53 <dr-noam hostname=""> command.</dr-noam>
	open between NOAM and	 Verify that the customer firewall is configured to allow DNS traffic on UDP/TCP port 53:
	each DR- NOAM site	[admusr@Icepick-NO-A ~]\$ sudo nmap -sTU -p 53 Icepick-DRNOAM-A
		Starting Nmap 5.51 (http://nmap.org) at 2018- 03-02 17:57 EST
		Nmap scan report for Icepick-DRNOAM-A (10.75.202.173)
		Host is up (0.00025s latency).
		rDNS record for 10.75.202.173: Icepick-DRNOAM- A.platform.cgbu.us.oracle.com PORT STATE SERVICE
		53/tcp open domain
		53/udp open domain
		MAC Address: 02:05:39:E0:60:8A (Unknown)
		Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds
		[admusr@Icepick-NO-A ~]\$
		If port is reported as any state other than "Open", then inform the Customer before accepting the upgrade.
		<i>Note</i> : If the ports are reported as "Closed" it may be because no services are running on the far end. Check with the Customer if the firewall has been configured to allow DNS traffic on port 53.
		If the port is reported as "Filtered" then the port is likely blocked by a Firewall and the upgrade MUST not be accepted until the Customer confirms that their network will allow DNS traffic on port 53.

Step #	Procedure	Description
2.	Verify if the	From the command prompt of the server with the alarm:
	UDP/TCP port 53 is	1. Issue the sudo nmap -sTU -p 53 <soam hostname=""> command.</soam>
	open between	 Verify the customer firewall is configured to allow DNS traffic on UDP/TCP port 53:
	NOAM and each SOAM site	[admusr@Icepick-NO-A ~]\$ sudo nmap -sTU -p 53 Icepick-SO-A
	Sile	Starting Nmap 5.51 (http://nmap.org) at 2018- 03-02 17:57 EST
		Nmap scan report for Icepick-SO-A (10.75.202.173)
		Host is up (0.00025s latency).
		rDNS record for 10.75.202.173: Icepick-SO- A.platform.cgbu.us.oracle.com
		PORT STATE SERVICE
		53/tcp open domain
		53/udp open domain
		MAC Address: 02:05:39:E0:60:8A (Unknown)
		Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds
		3. If port is reported as any state other than "Open" then inform the Customer before accepting the upgrade.
		Note: If the ports are reported as "Closed" it may be because no services are running on the far end. Verify with the Customer that the firewall has been configured to allow DNS traffic on port 53.
		4. If the port is reported as "Filtered" then the port is likely to be blocked by a firewall and the upgrade MUST not be accepted until the Customer confirms that their network will allow DNS traffic on port 53.
3. □	Verify if the UDP/TCP	 List the contents of the file /etc/resolv.conf via the "sudo cat etc/resolv.conf" command.
	port 53 is open between MP and each	 Verify that the Customer Firewall is configured to allow DNS traffic on UDP/TCP port 53 to the addressed from the file /etc/resolv.conf:
	name server of the	[admusr@Icepick-DAMP-1 ~]\$ sudo cat /etc/resolv.conf (lookups)
	/etc/resolv.c	domain platform.cgbu.us.oracle.com
	onf file	nameserver 10.240.50.134
		nameserver 10.240.50.133
		search platform.cgbu.us.oracle.com 5001ab.com
		labs.tekelec.com labs.nc.tekelec.com
		[admusr@Icepick-DAMP-1 ~]\$

Step #	Procedure	Description
		[admusr@Icepick-DAMP-1 ~]\$ sudo nmap -sTU -p 53 10.240.50.134 10.240.50.133
		Starting Nmap 5.51 (http://nmap.org) at 2018- 03-02 17:46 EST
		Nmap scan report for Icepick-SO-B- imi.platform.cgbu.us.oracle.com (10.240.50.134)
		Host is up (0.00022s latency). PORT STATE SERVICE
		53/tcp open domain
		53/udp open domain
		MAC Address: 02:17:B4:4F:DA:B6 (Unknown)
		Nmap scan report for Icepick-SO-A- imi.platform.cgbu.us.oracle.com (10.240.50.133)
		Host is up (0.00025s latency).
		PORT STATE SERVICE
		53/tcp open domain
		53/udp open domain
		MAC Address: 02:EE:13:E2:2C:EF (Unknown)
		Nmap done: 2 IP addresses (2 hosts up) scanned in 5.66 seconds
		[admusr@Icepick-DAMP-1 ~]\$
		If port is reported as any state other than "Open" then inform the Customer before accepting the upgrade.
		<i>Note</i> : If the ports are reported as "Closed" it may be because no services are running on the far end. Verify with the Customer that the firewall has been configured to allow DNS traffic on port 53.
		If the port is reported as "Filtered" then the port is likely to be blocked by a Firewall and the upgrade MUST not be accepted until the Customer confirms that their network will allow DNS traffic on port 53.

Appendix Q. Workaround to Resolve DB Site Replication Alarms

The following procedure resolves DB site replication alarms if encountered during the upgrade. Database (DB) replication failure alarms may display during an Auto Site Upgrade or during an event that resets multiple servers in parallel. The DB on the child servers is not updated until resolved.

Procedure 65. Workaround to Resolve DB Site Replication Alarms

Step #	Procedure	Description								
This pro	This procedure restarts the inetrep process on the server that has a DB replication failure alarm.									
Note:	te: All UI displays are sample representations of upgrade screens. The actual display may vary slightly.									
	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.									
If this pr	ocedure fails, it is	recommended to contact My Oracle Support (MOS) and ask for assistance.								
1.	Server CLI: Log into the server	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the active NOAM: ssh_admusr@ <server_address></server_address>								
		password: <enter password=""></enter>								
		Answer yes if you are asked to confirm the identity of the server.								
2.	Server CLI: Check if the replication links are up	Execute this command: irepstat Some of the B-C and C-C replications links may be down.								
3.	Server CLI: Resolve replication issue(s)	Execute this command: sudo pm.kill inetrep								
4. □	Repeat, if needed	Repeat procedure on each affected server								

Appendix R. Workaround to Resolve the Server HA Switchover Issue

The following procedure resolves the HA switchover issue.

Procedure 66. Resolve the HA Switchover Issue on Affected Server(s)

Step #	Procedure	Description					
 This procedure restarts the cmha process on the server that has HA switchover issue. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance. 							
1.	Server CLI: Log into the server	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the NOAM server which is experiencing the HA switchover issue : ssh admusr@ <server address=""> password: <enter password=""> Answer yes if you are asked to confirm the identity of the server.</enter></server>					
2.	Server CLI: Resolve HA switchover issue(s)	Execute this command: sudo pm.kill cmha					
3. □	Repeat, if needed	Repeat procedure on each affected server.					

Appendix S. Workaround to Resolve Device Deployment Failed Alarm

Procedure 67. Resolve Device Deployment Failed Alarm

Step #	Procedure	Description						
	This procedure is to resolve the device deployment failed alarm i.e. 10054							
Check c number.	Check off ($ sigma$) each step as it is completed. Boxes have been provided for this purpose under each step number.							
If this pr	ocedure fails, it is r	ecommended to contact My Oracle Support (MOS) and ask for assistance.						
1.		Open the web browser and enter a URL of:						
	GUI: Login	http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>						
		Log into the NOAM GUI as the guiadmin user:						
		ORACLE						
		Oracle System Login Tue Jun 7 13:49:06 2016 EDT						
		Log In Enter your username and password to log in						
		Username:						
		Password:						
		Change password						
		Log In						
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.						
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.						
		Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.						
2.		Navigate to current alarm details and identify the server and interface where the						
	GUI: Identify server(s) and	 10054 - Device Deployment Failed alarm is displayed. 1. Navigate to Alarms & Events > View Active. 						
	interface(s) with alarm	2. Look for the 10054 alarm make a list of the server(s) and interface(s).						

Step #	Procedure	Description
3.	NOAMP VIP GUI: Corrective	Interfaces like xmi and imi are in locked state and do not allow editing as a corrective action.
	action for alarm 10054	For xmi and imi interfaces, first unlock the interface and for other interfaces skip steps (a) to (d) below.
		 Navigate to Configuration > Networking > Networks, select the respective "Network element" tab used for the server configuration
		2. Click on the Network Name row.
		3. Click Unlock . Click on the checkbox to confirm it and click OK .
		 To unlock the network for the particular device, navigate to Configuration Networking > Devices.
		5. Click on the Server tab from the list in Step 2.
		 Select each interface row one by one for which alarm is showing and click Edit.
		7. Click OK .
		<i>Note</i> : Give some time to system to auto correct the condition to clear the alarm.
		Once this step is done, lock the network back again which were unlocked above.
		For xmi and imi interfaces, lock the interface back, for other interfaces skip (a) to (d) below.
		 To lock the network for a specific device, navigate to Configuration > Networking > Networks, select the respective Network element tab used for the server configuration.
		9. Click the Network Name row.
		10. Click Lock. Click on the checkbox to confirm it and click OK.

Appendix T. Workaround to Resolve syscheck Error for CPU Failure

Procedure 68. Workaround to Resolve syscheck Error for CPU Failure

Step #	Procedure	Description							
Workard	Workaround to resolve syscheck error for CPU failure.								
number	Check off ($\sqrt{1}$) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.								
1.	Log into the server using	Use the SSH command (on UNIX systems – or putty if running on windows) to log into the server identified.							
	CLI on which	ssh admusr@ <server_xmi></server_xmi>							
	syscheck is failing	password: <enter password=""></enter>							
	lainig	Answer yes if you are asked to confirm the identity of the server							
2.	Server CLI:	1. Edit the cpu config file.							
	Execute workaround	\$ sudo vim /usr/TKLC/plat/lib/Syscheck/modules/system/cpu/config							
		Comment out the all texts that reads: EXPECTED_CPUS= by putting # at the beginning of the line, for example:							
		# EXPECTED CPUS=2							
		3. Save the cpu config file.							
		4. Reconfig the syscheck by running these commands:							
		sudo syscheckunconfig							
		sudo syscheckreconfig							
		sudo syscheck							
		CPU related errors do not display.							

Appendix U. Create a Link for ComAgent

Procedure 69. Create a Link for ComAgent

Step #	Procedure	Description
This pro	cedure provides the	e details about creating a symbolic link of Comagent.
Note:	This procedure is e	xecuted only after all servers in the same server group are backed out.
Check o number.	• •	t is completed. Boxes have been provided for this purpose under each step
If this pr	ocedure fails, it is re	ecommended to contact My Oracle Support (MOS) and ask for assistance.
1.	Server CLI: Log into the	Use the SSH command (on UNIX systems – or putty if running on Windows) to log into the server under backout:
	server (if not	ssh admusr@ <server address=""></server>
	already done)	password: <enter password=""></enter>
		Answer yes if you are asked to confirm the identity of the server.
2.	Server: Create a	Execute the following commands to create a Comagent link:
	link for ComAgent	1. Navigate to /var/TKLC/appworks/library.
	oonn gent	<pre>\$ cd /var/TKLC/appworks/library</pre>
		2. Create a link
		<pre>\$ sudo ln -s /usr/TKLC/comagent-gui/gui/ Comagent</pre>
		Verify if the ComAgent link has been restored.
		[admusr@HPC-H01 library]\$ 1s -ltr
		total 56
		drwxr-xr-x 7 awadmin awadm 4096 Aug 25 2017 Diameter
		<pre>lrwxrwxrwx 1 root root 47 Dec 15 02:05 Zend -> /usr/T#LC/plat/www/zend-framework/library/Zend/</pre>
		lrwxrwxrwx 1 root root 21 Dec 15 02:07 Awpss? ->
		/usr/TKLC/awpss7/gui/ lrwxrwxrwx 1 root root 29 Dec 15 02:07 TransportHgr -> /usr/TKLC/awptransportmgr/gui
		<pre>irwsrwsrws 1 root root 38 Dec 15 02:07 Exgstack -> /usr/TKLC/awptransportmgr/gul/Exgstack</pre>
		drwxr-sr-s 3 awadmin awadm 4096 Dec 31 15:58 Rhar
		drwxr-xr-x 4 awadmin awadm 4096 May 22 10:#2 AWCLI
		drwxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Radius
		drwxr-xr-x 4 awadmin awadm 4096 May 22 10:44 Dca
		drwxr-wr-w 3 awadmin awadm 4096 May 22 10:44 Fabr
		drwxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Gla drwxr-xr-x 2 awadmin awadm 4096 May 22 10:44 Loadgen
		drwxr-wr-w 3 awadmin awadm 4096 May 22 10:44 Mapiwr
		drwxr-xr-x 6 awadmin awadm 4096 May 22 10:44 Fdra
		drwxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Sbr
		druxr-xr-x 3 awadmin awadm 4096 May 22 10:44 Vstp
		lrwxrwxrwx 1 root 18 May 22 10:44 Tpfe -> /usr/TRLC/ipfe/gui
		drwar-ar-a 3 awadmin awadm 4096 May 22 10:45 Cabr drwar-ar-a 17 awadmin awadm 4096 May 22 10:45 AppWorks
		drwxr-xr-x 17 awaimin awaimi Gose May 22 10:45 Appworks Irwxrwkrwx 1 root root 27 May 22 11:47 Comagent ->
		/usr/TRLC/consgent-gui/gui/
		If the output is received as highlighted in red, the softlink for Comagent
		directory has been restored.

Appendix V. Change SOAM VM Profile for Increased MP Capacity on an OpenStack system

Procedure 70. Change SOAM VM Profile for Increased MP Capacity on an OpenStack system

Step #	Procedure	Description												
Check o number.	cedure provides the ff (\checkmark) each step as it occedure fails, it is re-	is completed.	Box	kes have	e been pr	ovided	for t	this	pu	rpos	e un	der	each	-
1.	Log in to OpenStack	Log in to Oper	C	3	horizon c	dashbc	pard.							
2.	Identify and shut down the instance	Go to the corre from the list.		-	Instance	and se	elect	the	Sh	ut O	ff In	istai	nce	option
	motaneo	-Project	Instances											
		Compete			Instance Name	10. T 80AM				Film 4	a Launih In	inca	Contract in	Was Actins +
		N Strangton	a	Instance Name	Image Name	IP Address	Ser	Hey Pait	Status	Availabilit Zone	Task	Poner State-	Tarse since crusted	Active
		Volume Volume Arcan & Incolo	o	Desite (1944)	0158- 03038_0350+mmb	axt-rait 10.75.153.200 103 102.947.2.5	.00 2440		Arites	18(14)	Nota	Barring	1 manife 3 analta	Tracia Seasona (*) Associata Flucing (*) Malaki Manfara
		Notwork -	8	DurSwitti DAWIN	018- 53351_0350vmb	est-ret 10.75 103 554 152 157 2.4	de same		Arthre	10014	her	Revie	1 marti 1 marti	Colociti Interface Edit Interface Updata Metadate Edit Security Grauga Caronite
		Adada -	8	b-shannawin	1006- 030331_0030venth	ити 190 107.2.50 ast-not 10.75.162.50	acom		Buicf	70018	line	Diwi Dave	4 marij 7 marij	Manut.og Pause Indance Skipord Pytania Shehe Indance Havite Indance
				Defensioner	1588 53333_13350.vmds	intii 152 107 3 8 ext-net 10 75 152 230	-		livent	10214	Nora	Stari Durit	f turk Turak	Lenit Instance Unlock Instance Self Related Instance Mart Of Instance Relat Of Instance Relativit Instance

Step #	Procedure	Description										
3.	Resize instance	Once the insta the list:	instance is in Shutoff state, select the Resize Instance option from									
		-Propet	Instances									
		Computer -		Instalice Marrie	1			. Ether	ALAUNI		a lamente	Ware Actions +
		Dynayshop	C Instance Name	image Name	IP Address	Ser	Key Status	Analasi Zune	ity Test	Poster	Timpi shice	Active
		toptantes					1575				counted	
		Walance Seager	0 praescover	11NA. 03033_0150 cmdb	400-040 10.25.153.200 100 100.467.2.5	-	- Ada		Nora	Barity	S months S presides	n Create Assested (*) Associate Floating P
		Acres & Secolg	C DAMAGONAN	00A- 03000_030vm8	4027-1440 10.75-102-164 1091 192-907-5-4	-	- Advi	-	here	Ranning	l vati 1 vet	Attach Analipse Detects Interfecte Edit Interfecte Update Metadate Edit Security Groups
		Admin - Monthy -	o pessational	008. 83333,030.008	1177 196 407.2.90 est-net 10.75 192.50	de sure	- Date	10010	Tires.	Unit Dave	i nati Tanti	Consule View Log Pause Instance Stargerd Instance Starles Instance Ratigs Instance
			C Determinant	1999- 1933 8_6330 vents	HTE 192.107.2.9 ext-net 10.75.152.230		- Sad		Sires	Bhel Dison	4 marti 1 marti	Lock Patience Lowood Roberts Soft/Satient Instance Yourd Robert Instance That Of Instance Hade do Instance
	VCPUs size and memory configuration	Resize Instance	Flavor	Details								
		dir soam		Name								
		New Flavor * Ø		VCPU	e.							
		Select a New Flame		.+ Root D	(ak	- 13	JB					
		Bakect a New Flavor		Epitama		- 24	GB					
		KLI		Total D	Total Disk.		GB					
		mit ling alapar ven		RAM		1	RES					
		mit annall TG faich radod.hm		1.1.2-5.21	t Limits of Instances	: 26 of 100		(2004)	-			
		ebervala diseby		Number	Number of VCPUs 225 of 400 Union							
				Total RA	M		o Aline of the	1.206-540	-			
		pic acquisitionnap derSp-30 tric acquisition					Cancel	Res	den :			
			i ze . formation c DSR Cloud						ze a	nd m	nemo	ory, refer

Appendix W. Change SOAM VM Profile for Increased MP Capacity on a VMware system

Step #	Procedure	Description						
	cedure describes he							off (\Box) each
If this pro	ocedure fails, it is re	ecommended to	contact N	ly Orac	le Sup	port (MOS) and ask for as	sistance.
1.	Log in to Active NOAM	2. Navig 3. Confir 4. Identif	ate to Mai m that at y the Action ole" colum	n Menu least or ve and	u > Sta ne SO	by SOAM s		
		ACHAR B BOAM A	684 684	tas.	Ame Ame	140444.8 004448	HDMI SOAN	Numeric GAMAP
		954M-8 3854	Dands Adva	194	Oarstv Adve	SOMLA MP-2	5048 5048	Surger DAB
		69-2 1975-41	Dande:	005	Active Active	ar.1	514 214	
		167-1	kdre .	iche	Active		8044	
2.	Check System Alarms	2. Confir syster 3. In cas and re	m that the n health, o e of any a	ere are or SOA larms, m, and	no ala Ms. stop tł	rms related	ts > View Active I to Replication, identify the caus the next steps v	Merging, se of alarms,
3.	Take Standby SOAM out of service in HA	2. Press 3. Take Role of 4. Press Inform Not C 5. Press The s now S	the Edit k the SOAM of OOS. OK. nation disp ommitted" OK. ystem goe howing O	outton i 1 identif olays in 2. es back 0OS in '	n lowe fied as format to the 'Max A	Standby ir ion banner previous s llowed HA	age > HA. r of the page. step 1 to Max "Pre-Validation creen with the S Role" and "OAI rned off for any	passed-Data Standby SOAM M HA Role".
				Main Menu	r: Status & M	lanage → HA (Edit)		
				100° -				
				Medifying	HA attributes			
				Heatharias M	or Allowed AA (Inde			
				HIME .	Caroline .	The maximum and will HA Run	a foo rystaataa.	
				10468	100	The maintain exercise 444 fills	e for reliefe al	
				SIMPA A	ide :	The reading of the reading of the Read	nto Ulima	
				-	006	The maximum desired HL Rei	n for (90444.0)	
4.	Stop/Shut down the VM		to Comm				e SOAM taken o	out of service.

Step #	Procedure	Description
5.	Modify the vCPU and Memory	 NOTE: Depending upon the VM manager, the exact steps may be different. Contact your VM manager for any help on the exact steps. 1. Confirm that the virtual machine is powered off. 2. Click the virtual machine. 3. Go to Settings. 4. Edit System Settings to change: a. vCPU: 8 b. RAM/Base Memory: 14,336 (14GB, 14 x 1024)
6. □	Start the VM	 Set Power State of VM to Power ON in the VM Manager and wait for a few minutes.
7.	Log in to SOAM using CLI	 Use the SSH command to log in to the respective SOAM identified. ssh admusr@<server_xmi> password: <enter password=""></enter></server_xmi> Answer yes when prompted to confirm the identity of the server.
8.	Confirm that the SOAM is showing 8 vCPU	1. On the SOAM CLI, execute the mpstat -P ALL command. The output should be one line for each vCPU. Confirm that for vCPU=8, the output shows 8 lines: [admusr@labSOAM ini]\$ mpstat -P ALL Linux 2.6.32-573.26.1.el6prerel7.0.3.0.0_86.46.0.x86_64 (guruDSR-N01) 05/01/2020 _x86_64_ (8 CPU) 06:31:04 AM CPU %usr %nice %sys %iowait %irq %soft %steal %guest %idle 06:31:04 AM all 0.72 0.30 0.39 0.03 0.00 0.00 0.10 0.00 98.46 06:31:04 AM 0 0.67 0.52 0.44 0.26 0.00 0.00 0.11 0.00 97.99 06:31:04 AM 1 0.85 0.22 0.47 0.00 0.00 0.00 0.00 98.36 06:31:04 AM 2 0.56 0.48 0.38 0.00 0.00 0.00 0.09 98.48 06:31:04 AM 3 0.58 0.22 0.35 0.00 0.00 0.00 0.09 98.73 06:31:04 AM 4 0.55 0.26 0.36 0.00 0.00 0.00 0.09 98.73 06:31:04 AM 5 1.44 0.18 0.40 0.00 0.00 0.00 0.11 0.00 97.86 06:31:04 AM 6 0.53 0.22 0.35 0.00 0.00 0.00 0.09 98.81 06:31:04 AM 7 0.53 0.29 0.38 0.00 0.00 0.00 0.08 0.00 98.71
9.	Check memory (RAM) size is 14 GB	<pre>1. On the SOAM CLI, execute the following command: cat /proc/meminfo vmstat -s Sample output: admusr@labNOAM ini]\$ cat /proc/meminfo MemTotal: 14007172 kB [admusr@labNOAM ini]\$ vmstat -s 14007172 total memory</pre>
10.	Increase measurement memory and queue size	 Execute the following command: sudo sh /usr/TKLC/dsr/prod/maint/loaders/install/load.AppwMeasMem Verify if the MeasMem.inifile is created for measurement memory size of 3072 MB: cat /var/TKLC/appworks/ini/MeasMem.ini Note: INI entry should be aw.measure.maxmem = 3072 Verify that the measurement queue size is set to 2 in LongParam table where the parameter name "measurementMaxQueues" is 2: iqt -pE LongParam grep measurementMaxQueues

Step #	Procedure	Description							
11.	Bring back SOAM in to service	 Log in to the Active NOAM GUI using the VIP. Navigate to Main Menu > Status & Manage > HA. Press the Edit button in the lower-left corner of the page. Take the modified SOAM to Max Allowed HA Role of "ACTIVE". War Man Barry & Hallow & Manage + HA [50] War Manage + HA [50] Mar Manage + HA [50]							
12.	Take ACTIVE SOAM out of service in HA	 Navigate to Main Menu > Status & Manage > HA. Press the Edit button in the lower-left corner of the page. Take the SOAM identified as ACTIVE in Step 1 to Max Allowed HA Role of OOS. Press OK. Information displays the information banner "Pre-Validation passed- Dat Not Committed". Press OK. The system goes back to the previous screen with the ACTIVE SOAM showing OOS in "Max Allowed HA Role" and "OAM HA Role". Confirm that the SOAM that was Standby earlier is now ACTIVE in "Max Allowed HA Role" and "OAM HA Role". At this point, the server is ready to be turned off for any change. 							
13. □	Repeat on Active SOAM VM	Repeat Step 4 to 11 on the SOAM VM.							

Appendix X. Reset the SOAP Password

Procedure 72. Reset the SOAP Password

Step#	Procedure	Description		
following	This procedure provides the details about resetting the SOAP password. When Oracle is upgraded, the following procedure resets the SOAP password, for the DSR to perform self-authenticate with IDIH.			
Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.				
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	Login to NOAM: Login on the active NOAM server	 Login as admusr on the active NOAM server. Retrieve the TPD web service password in plaintext by executing: \$ /usr/TKLC/appworks/bin/aw.wallet credential get cmsoapa password 		
		The command will print the current plaintext configuration web service password.		
		For example: 7w57q9U00v0tKtgtLVTMajDcXfhCj2F4nyXw45qK6EXNHA9jACyQ		
2.	Login to the	1. Login as admusr on the IDIH application server.		
	IDIH application server	 2. Change the user to tekelec by executing: sudo su - tekelec 3. Reset/Create the Configuration web service password: a. Go to the directory /usr/TKLC/xIH/apps/trace-refdata-adapter/ b. run ./resetSoapPassword.sh c. When prompted for password: <enter from="" obtained="" password="" step1.2="" the=""></enter> Note: This script prints the encrypted password. The new encrypted SOAP password is stored into IDIH Oracle database. 4. Verify if the password is stored in IDIH Oracle database by executing: a. sqlplus /@NSP b. Select * from DSR_USER_CREDENTIALS; Here you should see the same encrypted password as in Step 2.3. c. Type exit to exit from database. 		
		<pre>WebLogic application server must be restarted on IDIH application server. a. Become admusr by executing: exit b. Stop the WebLogic application server by executing: sudo service xih-apps stop c. Start the WebLogic application server by executing: sudo service xih-apps start The Weblogic server might take few minutes to resume its service. Note: Upon completion of the above steps, in IDIH /var/TKLC/xIH/log/apps/weblogic/apps/application.log file you should see NO Error.</pre>		

Appendix Y. Restore the Servers with Backout Errors

Procedure 73. Restore the Servers with Backout Errors

Step#	Procedure	Description	
This workaround resolves a backout failure error. Execute this procedureon the failed server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	Identify the rpm	Recognize the rpm (dsr/dpi) which yielded the scriptlet failure. Examine the upgrade log at /var/TKLC/log/upgrade/upgrade.log for errors that occurred during the backout. \$ rpm -qa <rpm_name> Example: \$ rpm - qa <tklcdsr.x86_64> Note: There will be two rpms, identify the newer rpm.</tklcdsr.x86_64></rpm_name>	
2. □	Uninstall the rpm	Uninstall the newer version of the rpm: rpm -e <rpm_name></rpm_name>	
3.	Identify the rpm	Execute this command: \$ rpm -qa <rpm_name> Note: There must be a single rpm.</rpm_name>	
4. □	Restore the database	Run the sudo /var/tmp/backout_restore command to restore the database and restart the server.	

Appendix Z. My Oracle Support (MOS)

My Oracle Support

MOS (<u>https://support.oracle.com</u>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <u>http://www.oracle.com/us/support/contact/index.html</u>. When calling, make the selections in the sequence shown on the Support telephone menu:

- 1. Select 2 for New Service Request.
- 2. Select 3 for Hardware, Networking and Solaris Operating System Support.
- 3. Select one of the following options:

For technical issues such as creating a new Service Request (SR), select 1.

For non-technical issues such as registration or assistance with MOS, select 2.

You are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, and 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at 1–800–223–1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- · Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

- 1. Access the **Oracle Help Center** site at http://docs.oracle.com.
- 2. Click Industries.
- 3. Under the Oracle Communications subheading, click the Oracle Communications documentation link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings Network Session Delivery and Control Infrastructure or "Platforms."

4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.